PATENT
8022-1063

IN THE U.S. PATENT AND TRADEMARK OFFICE

In re application of: Kazuya SUZUKI et al.
Conf.:
Appl. No.: NEW NON-PROVISIONAL
Group:
Filed: November 17, 2003
Examiner:
Title: KEY MANAGEMENT SYSTEM AND MULTICAST DELIVERY SYSTEM USING THE SAME

CLAIM TO PRIORITY

Assistant Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

November 17, 2003

Sir:

Applicant(s) herewith claim(s) the benefit of the priority filing date of the following application(s) for the above-entitled U.S. application under the provisions of 35 U.S.C. § 119 and 37 C.F.R. § 1.55:

Country	Application No.	Filed
JAPAN	2002-332405	November 15, 2002
JAPAN	2002-332404	November 15, 2002
JAPAN	2002-335401	November 19, 2002

Certified copy(ies) of the above-noted application(s) is(are) attached hereto.

Respectfully submitted,

YOUNG & THOMPSON

Benoit Castel

Benoit Castel, Reg. No. 35,041

745 South 23rd Street
Arlington, VA 22202
Telephone (703) 521-2297

BC/yr

Attachment(s): 3 Certified Copy(ies)

併合親2002-332404
US
924

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００２年１１月１５日

出 願 番 号
Application Number: 特願２００２－３３２４０５

[ST. 10/C]: [ＪＰ２００２－３３２４０５]

出 願 人
Applicant(s): 日本電気株式会社
日本電気通信システム株式会社

２００３年 ９月２５日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号 出証特２００３－３０７８９５０

【書類名】　特許願
【整理番号】　49200233
【あて先】　特許庁長官殿
【国際特許分類】　H04L　9/08
H04L 12/56
G06F 13/00
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　鈴木　一哉
【発明者】
【住所又は居所】　東京都港区三田一丁目４番２８号　日本電気通信システム株式会社内
【氏名】　馬越　英之
【発明者】
【住所又は居所】　東京都港区芝五丁目７番１号　日本電気株式会社内
【氏名】　地引　昌弘
【特許出願人】
【識別番号】　000004237
【氏名又は名称】　日本電気株式会社
【特許出願人】
【識別番号】　000232254
【氏名又は名称】　日本電気通信システム株式会社
【代理人】
【識別番号】　100088890
【弁理士】
【氏名又は名称】　河原　純一
【手数料の表示】
【予納台帳番号】　009690
【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9001717

【包括委任状番号】　9002497

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　マルチキャスト配信のための鍵管理方式

【特許請求の範囲】

【請求項１】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

コンテンツサーバ群とクライアント群とからアクセス可能となるように配置されており、暗号鍵・復号鍵と当該鍵を一意に識別するための鍵ＩＤとの組を保持することによって鍵を管理する鍵管理サーバと、

前記鍵管理サーバから暗号鍵とその鍵ＩＤとの組を受け取り、当該暗号鍵で暗号化されたデータと当該鍵ＩＤとを有するマルチキャストパケットをクライアント群に送信するコンテンツサーバと、

前記コンテンツサーバからマルチキャストパケットを受信し、当該マルチキャストパケットに含まれる鍵ＩＤに対応する復号鍵を前記鍵管理サーバから取得し、当該復号鍵によって当該マルチキャストパケットに含まれる暗号化データの復号化を行うクライアントと

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項２】　鍵管理サーバを鍵管理マスタサーバと複数の鍵管理スレーブサーバとに分けることによって、負荷分散を可能にすることを特徴とする請求項１記載のマルチキャスト配信のための鍵管理方式。

【請求項３】　コンテンツサーバが、使用する鍵を変更するときに、事前に鍵変更予告のマルチキャスト配信を行い、鍵管理サーバからの新たな復号鍵の取得をクライアントに促すことによって、鍵変更時にも遅延なく復号化を行うことを可能にすることを特徴とする請求項１または請求項２記載のマルチキャスト配信のための鍵管理方式。

【請求項４】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

暗号鍵・復号鍵と当該鍵を一意に区別するための鍵ＩＤとの組を保持する鍵管理サーバ内の鍵管理テーブルと、

コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該

鍵に鍵ＩＤを割り当て、生成した暗号鍵・復号鍵と当該鍵ＩＤとの組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵ＩＤとの組を有する鍵情報応答メッセージを当該コンテンツサーバに返送する鍵管理サーバ内の鍵生成手段と、

クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵ＩＤに対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵ＩＤとの組を有する鍵情報メッセージを当該クライアントに返送する鍵管理サーバ内の復号鍵送付手段と、

暗号鍵とその鍵ＩＤとの組を保持するコンテンツサーバ内の暗号鍵テーブルと、

マルチキャスト配信時に、暗号鍵を取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵ＩＤとの組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、

前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットの送信を行うコンテンツサーバ内の暗号化・送信手段と、

復号鍵とその鍵ＩＤとの組を保持するクライアント内の復号鍵テーブルと、

マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵ＩＤに対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には鍵管理サーバに対して当該鍵ＩＤをキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵ＩＤとの組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、

マルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段と

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項５】　暗号化データのマルチキャスト配信が行われるネットワークシス

テムにおいて、'

暗号鍵・復号鍵と当該鍵を一意に区別するための鍵ＩＤとの組を保持する鍵管理マスタサーバおよび鍵管理スレーブサーバ内の鍵管理テーブルと、

コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵ＩＤを割り当て、生成した暗号鍵・復号鍵と当該鍵ＩＤとの組を鍵管理マスタサーバ内の前記鍵管理テーブルに保存し、当該暗号鍵とその鍵ＩＤとの組を有する鍵情報応答メッセージを当該コンテンツサーバに返送し、当該暗号鍵・復号鍵と当該鍵ＩＤとの組を有する鍵情報配布メッセージを全ての鍵管理スレーブサーバに配布する鍵管理マスタサーバ内の鍵生成・配布手段と、

前記鍵生成・配布手段によって配布された鍵情報配布メッセージ中の暗号鍵・復号鍵と鍵ＩＤとの組を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルに保存する鍵管理スレーブサーバ内の鍵保存手段と、

クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵ＩＤに対応する鍵を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵ＩＤとの組を有する鍵情報メッセージを当該クライアントに返送する鍵管理スレーブサーバ内の復号鍵送付手段と、

暗号鍵とその鍵ＩＤとの組を保持するコンテンツサーバ内の暗号鍵テーブルと、

マルチキャスト配信時に、暗号鍵を取得するために鍵管理マスタサーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵ＩＤとの組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、

前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットの送信を行うコンテンツサーバ内の暗号化・送信手段と、

復号鍵とその鍵ＩＤとの組を保持するクライアント内の復号鍵テーブルと、

マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵ＩＤに対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には全ての鍵管理スレーブサ

ーバのいずれかに対して当該鍵ＩＤをキーにした鍵情報要求を送信し、その鍵情報要求の返信として当該鍵管理スレーブサーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵ＩＤとの組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、

マルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段と

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項６】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

暗号鍵・復号鍵と当該鍵を一意に区別するための鍵ＩＤとの組を保持する鍵管理サーバ内の鍵管理テーブルと、

コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵ＩＤを割り当て、生成した暗号鍵・復号鍵と当該鍵ＩＤとの組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵ＩＤとの組を有する鍵情報応答メッセージを当該コンテンツサーバに返送する鍵管理サーバ内の鍵生成手段と、

クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵ＩＤに対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵ＩＤとの組を有する鍵情報メッセージを当該クライアントに返送する鍵管理サーバ内の復号鍵送付手段と、

暗号鍵とその鍵ＩＤとの組を保持するコンテンツサーバ内の暗号鍵テーブルと、

鍵変更準備時点に達した時に、次に使用する暗号鍵を事前に取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵ＩＤとの組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、

前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットの送信を行うコンテンツサーバ内の暗号化・送信手段と、

前記暗号鍵取得手段によって次に使用する暗号鍵の取得が行われた場合に、当該暗号鍵の鍵ＩＤを有する鍵変更予告メッセージのマルチキャスト配信を行うコンテンツサーバ内の鍵変更予告手段と、

復号鍵とその鍵ＩＤとの組を保持するクライアント内の復号鍵テーブルと、

鍵変更予告メッセージの受信時に、当該鍵変更予告メッセージ中の鍵ＩＤに対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がない場合に鍵管理サーバに対して当該鍵ＩＤをキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵ＩＤとの組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、

マルチキャストパケットを受信し、前記復号鍵取得手段により事前に取得され前記復号鍵管理テーブルに保持されており当該マルチキャストパケット中の鍵ＩＤに対応する復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段と

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項７】　コンテンツサーバ側で、複数の暗号鍵と鍵ＩＤとの組を同時に保持しており、マルチキャスト配信において使用する暗号鍵を適時変更することを可能ならしめることを特徴とする請求項１，請求項２，請求項３，請求項４，請求項５，または請求項６記載のマルチキャスト配信のための鍵管理方式。

【請求項８】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

鍵管理サーバを、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵ＩＤとの組を保持する鍵管理テーブル，コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵ＩＤを割り当て、生成した暗号鍵・復号鍵と当該鍵ＩＤとの組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵ＩＤとの組を有する鍵情報応答メッセージを当該コンテンツサーバに返送する鍵生成手段，およびクライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵ＩＤに対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵ＩＤとの組を有する鍵情報メッセージを当該クライアントに返送する復号鍵送付手段とし

て機能させるための鍵管理サーバ用鍵管理プログラムと、
コンテンツサーバを、暗号鍵とその鍵ＩＤとの組を保持する暗号鍵テーブル，マルチキャスト配信時に、暗号鍵を取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵ＩＤとの組を前記暗号鍵テーブルに保存する暗号鍵取得手段，および前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットの送信を行う暗号化・送信手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、
クライアントを、復号鍵とその鍵ＩＤとの組を保持する復号鍵テーブル，マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵ＩＤに対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には鍵管理サーバに対して当該鍵ＩＤをキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵ＩＤとの組を前記復号鍵テーブルに保存する復号鍵取得手段，およびマルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行う受信・復号化手段として機能させるためのクライアント用鍵管理プログラムと
を有することを特徴とするマルチキャスト配信のための鍵管理方式。
【請求項９】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、
鍵管理マスタサーバを、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵ＩＤとの組を保持する鍵管理テーブル，およびコンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵ＩＤを割り当て、生成した暗号鍵・復号鍵と当該鍵ＩＤとの組を鍵管理マスタサーバ内の前記鍵管理テーブルに保存し、当該暗号鍵とその鍵ＩＤとの組を有する鍵情報応答メッセージを当該コンテンツサーバに返送し、当該暗号鍵・復号鍵と当該鍵ＩＤとの組を有する鍵情報配布メッセージを全ての鍵管理スレーブサーバに配布する鍵生成・配布手段と

して機能させるための鍵管理マスタサーバ用鍵管理プログラムと、
鍵管理スレーブサーバを、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵ＩＤとの組を保持する鍵管理テーブル，前記鍵生成・配布手段によって配布された鍵情報配布メッセージ中の暗号鍵・復号鍵と鍵ＩＤとの組を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルに保存する鍵保存手段，およびクライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵ＩＤに対応する鍵を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵ＩＤとの組を有する鍵情報メッセージを当該クライアントに返送する復号鍵送付手段として機能させるための鍵管理スレーブサーバ用鍵管理プログラムと、
コンテンツサーバを、暗号鍵とその鍵ＩＤとの組を保持する暗号鍵テーブル，マルチキャスト配信時に、暗号鍵を取得するために鍵管理マスタサーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵ＩＤとの組を前記暗号鍵テーブルに保存する暗号鍵取得手段，および前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットの送信を行う暗号化・送信手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、
クライアントを、復号鍵とその鍵ＩＤとの組を保持する復号鍵テーブル，マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵ＩＤに対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には全ての鍵管理スレーブサーバのいずれかに対して当該鍵ＩＤをキーにした鍵情報要求を送信し、その鍵情報要求の返信として当該鍵管理スレーブサーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵ＩＤとの組を前記復号鍵テーブルに保存する復号鍵取得手段，およびマルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行う受信・復号化手段として機能させるためのクライアント用鍵管理プログラムと

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【請求項１０】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、

鍵管理サーバを、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵ＩＤとの組を保持する鍵管理テーブル，コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵ＩＤを割り当て、生成した暗号鍵・復号鍵と当該鍵ＩＤとの組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵ＩＤとの組を有する鍵情報応答メッセージを当該コンテンツサーバに返送する鍵生成手段，およびクライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵ＩＤに対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵ＩＤとの組を有する鍵情報メッセージを当該クライアントに返送する復号鍵送付手段として機能させるための鍵管理サーバ用鍵管理プログラムと、

コンテンツサーバを、暗号鍵とその鍵ＩＤとの組を保持する暗号鍵テーブル，鍵変更準備時点に達した時に、次に使用する暗号鍵を事前に取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵ＩＤとの組を前記暗号鍵テーブルに保存する暗号鍵取得手段，前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットの送信を行う暗号化・送信手段，および前記暗号鍵取得手段によって次に使用する暗号鍵の取得が行われた場合に、当該暗号鍵の鍵ＩＤを有する鍵変更予告メッセージのマルチキャスト配信を行う鍵変更予告手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、

クライアントを、復号鍵とその鍵ＩＤとの組を保持する復号鍵テーブル，鍵変更予告メッセージの受信時に、当該鍵変更予告メッセージ中の鍵ＩＤに対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がない場合に鍵管理サーバに対して当該鍵ＩＤをキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵ＩＤとの組を前記復号鍵テーブルに保存する復号鍵取得手段，お

よびマルチキャストパケットを受信し、前記復号鍵取得手段により事前に取得され前記復号鍵管理テーブルに保持されており当該マルチキャストパケット中の鍵ＩＤに対応する復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行う受信・復号化手段として機能させるためのクライアント用鍵管理プログラムと

を有することを特徴とするマルチキャスト配信のための鍵管理方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて暗号化／復号化で用いられる鍵（暗号鍵／復号鍵）の管理を行うマルチキャスト配信のための鍵管理方式に関する。

【０００２】

【従来の技術】

ユニキャスト通信における暗号化データの通信のためのプロトコルとして、ＩＰｓｅｃ等があるが、これらはそのままではマルチキャスト通信（配信）には適用できない。ユニキャスト通信は一対一で行われるため、二者間で鍵を共有すればよいが、マルチキャスト通信では一対多の通信になるため、ユニキャスト通信と同じ方法では鍵の共有ができないからである。このため、マルチキャスト通信における暗号化では、ユニキャスト通信におけるそれとは別のしくみが必要になる。

【０００３】

一般に、複数のマルチキャスト配信が行われている場合に、それぞれを区別するためには、送信元アドレス，マルチキャストアドレス，および送受信ポート番号の組合せによって、その区別が行われている。

【０００４】

したがって、従来の技術では、コンテンツサーバが複数あり、それぞれが違う鍵を用いて暗号化されたデータを含むマルチキャストパケットを配信している場合において、クライアント側では、それぞれのマルチキャストパケットに対応した

復号鍵を得るために、送信元アドレス，マルチキャストアドレス，および送受信ポート番号の組合せでマルチキャストパケットを区別する必要があった。

【０００５】

また、暗号化データ（暗号化されたデータ）のマルチキャスト配信中に鍵（暗号鍵・復号鍵）を変える場合には、なんらかの方法を用いて、コンテンツサーバとクライアントとの間で、使用している暗号鍵・復号鍵の同期をとる必要がある。

【０００６】

ここで、従来の技術では、鍵の同期を行う方式として、次のような処理を行う鍵管理サーバを利用して当該同期を実現するシステムが存在した（例えば、特許文献１参照）。

【０００７】

すなわち、特許文献１に記載された鍵管理サーバは、送信者（コンテンツサーバ）が送信を始める際か鍵を変更した際に新しい鍵を受け取り、それを受信者（クライアント）に対して通知することで、送信データ（配信対象のデータ）に対応する鍵を受信者に配布している。

【０００８】

【特許文献１】

特開２００２－１１１６４９号公報（第４－５頁、図１）

【０００９】

【発明が解決しようとする課題】

上述した従来のマルチキャスト配信のための鍵管理方式には、鍵が変更された際に、鍵管理サーバがクライアントに対して新しい鍵を配布する必要があり、このような鍵の管理を実現するために、現時点でマルチキャストパケット受信中のクライアントを鍵管理サーバが把握しておく必要がある等、鍵の管理が煩雑になるという問題点があった。

【００１０】

本発明の目的は、上述の点に鑑み、マルチキャスト配信時に暗号化処理を行うネットワークシステムにおいて、事前に複数の鍵（暗号鍵・復号鍵）を一意に区別するための鍵ＩＤ（送信者（コンテンツサーバ）と多数の受信者（クライアント

）との間で共有する鍵を区別するＩＤ（ＩＤｅｎｔｉｆｉｃａｔｉｏｎ））を鍵毎に割り当てておき、マルチキャスト配信の際に、配信対象のデータの暗号化に用いた鍵に対応する鍵ＩＤをマルチキャストパケットに包含して送り、そのような鍵ＩＤを使用して鍵の管理を実現することによって、鍵の管理を容易に行うことを可能にするマルチキャスト配信のための鍵管理方式を提供することにある。

【００１１】

すなわち、本発明を用いれば、コンテンツサーバが暗号鍵を変えた時に、コンテンツサーバが暗号化データに添付する鍵ＩＤを変えるだけで、クライアントは受信したマルチキャストパケット中の鍵ＩＤをみることによって、暗号化・復号化に用いる鍵が変わったことを知ることができ、クライアント側から鍵管理サーバ側に新しい鍵を要求できるため、鍵管理サーバ側でクライアントに関する情報を管理する必要がなくなる。

【００１２】

なお、ＩＰｓｅｃ等のプロトコル（ユニキャスト通信のためのプロトコル）でも複数の鍵を区別するためにＩＤが用いられるが、それはあくまでも二者間で共有されている鍵を区別するためのものである。

【００１３】

また、ＰＫＩ（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ）を用いたＩＰｓｅｃ通信では公開鍵をＣＡ（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ）局と呼ばれるサーバにて保存しておき、クライアントが通信に先だってサーバから公開鍵を取得するということが行われるが、この公開鍵は通信のための共有鍵を交換するために用いられており、その公開鍵を使って暗号化通信を行うわけではない（本発明では、復号鍵およびその鍵ＩＤが鍵管理サーバからクライアントに渡される）。

【００１４】

【課題を解決するための手段】

本発明のマルチキャスト配信のための鍵管理方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵・復号鍵（対となる暗号鍵および復号鍵。同じ鍵である場合もある）と当該鍵を一意に区別するため

の鍵ＩＤとの組を保持する鍵管理サーバ内の鍵管理テーブルと、コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵ＩＤを割り当て、生成した暗号鍵・復号鍵と当該鍵ＩＤとの組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵ＩＤとの組を有する鍵情報応答メッセージを当該コンテンツサーバに返送する鍵管理サーバ内の鍵生成手段と、クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵ＩＤに対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵ＩＤとの組を有する鍵情報メッセージを当該クライアントに返送する鍵管理サーバ内の復号鍵送付手段と、暗号鍵とその鍵ＩＤとの組を保持するコンテンツサーバ内の暗号鍵テーブルと、マルチキャスト配信時に、暗号鍵を取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵ＩＤとの組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットの送信を行うコンテンツサーバ内の暗号化・送信手段と、復号鍵とその鍵ＩＤとの組を保持するクライアント内の復号鍵テーブルと、マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵ＩＤに対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には鍵管理サーバに対して当該鍵ＩＤをキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵ＩＤとの組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、マルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段とを有する。

【００１５】

ここで、本発明のマルチキャスト配信のための鍵管理方式は、上記の鍵管理サーバを、上記の鍵管理テーブル，鍵生成手段，および復号鍵送付手段として機能させるための鍵管理サーバ用鍵管理プログラムと、上記のコンテンツサーバを、上

記の暗号鍵テーブル，暗号鍵取得手段，および暗号化・送信手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、上記のクライアントを、上記の復号鍵テーブル，復号鍵取得手段，および受信・復号化手段として機能させるためのクライアント用鍵管理プログラムとを有する態様で実現することも可能である。

【００１６】

また、本発明のマルチキャスト配信のための鍵管理方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵ＩＤとの組を保持する鍵管理マスタサーバおよび鍵管理スレーブサーバ内の鍵管理テーブルと、コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵ＩＤを割り当て、生成した暗号鍵・復号鍵と当該鍵ＩＤとの組を鍵管理マスタサーバ内の前記鍵管理テーブルに保存し、当該暗号鍵とその鍵ＩＤとの組を有する鍵情報応答メッセージを当該コンテンツサーバに返送し、当該暗号鍵・復号鍵と当該鍵ＩＤとの組を有する鍵情報配布メッセージを全ての鍵管理スレーブサーバに配布する鍵管理マスタサーバ内の鍵生成・配布手段と、前記鍵生成・配布手段によって配布された鍵情報配布メッセージ中の暗号鍵・復号鍵と鍵ＩＤとの組を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルに保存する鍵管理スレーブサーバ内の鍵保存手段と、クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵ＩＤに対応する鍵を自己が存在する鍵管理スレーブサーバ内の前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵ＩＤとの組を有する鍵情報メッセージを当該クライアントに返送する鍵管理スレーブサーバ内の復号鍵送付手段と、暗号鍵とその鍵ＩＤとの組を保持するコンテンツサーバ内の暗号鍵テーブルと、マルチキャスト配信時に、暗号鍵を取得するために鍵管理マスタサーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵ＩＤとの組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットの送信を行うコンテンツサーバ

内の暗号化・送信手段と、復号鍵とその鍵ＩＤとの組を保持するクライアント内の復号鍵テーブルと、マルチキャストパケットの受信時に、当該マルチキャストパケット中の鍵ＩＤに対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がある場合にはその復号鍵を取得し、該当する復号鍵がない場合には全ての鍵管理スレーブサーバのいずれかに対して当該鍵ＩＤをキーにした鍵情報要求を送信し、その鍵情報要求の返信として当該鍵管理スレーブサーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵ＩＤとの組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、マルチキャストパケットを受信し、前記復号鍵取得手段により取得された復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段とを有するように構成することも可能である。

【００１７】

ここで、本発明のマルチキャスト配信のための鍵管理方式は、上記の鍵管理マスタサーバを、上記の鍵管理テーブルおよび鍵生成・配布手段として機能させるための鍵管理マスタサーバ用鍵管理プログラムと、上記の鍵管理スレーブサーバを、上記の鍵管理テーブル，鍵保存手段，および復号鍵送付手段として機能させるための鍵管理スレーブサーバ用鍵管理プログラムと、上記のコンテンツサーバを、上記の暗号鍵テーブル，暗号鍵取得手段，および暗号化・送信手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、上記のクライアントを、上記の復号鍵テーブル，復号鍵取得手段，および受信・復号化手段として機能させるためのクライアント用鍵管理プログラムとを有する態様で実現することも可能である。

【００１８】

さらに、本発明のマルチキャスト配信のための鍵管理方式は、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、暗号鍵・復号鍵と当該鍵を一意に区別するための鍵ＩＤとの組を保持する鍵管理サーバ内の鍵管理テーブルと、コンテンツサーバから鍵作成要求を受け取ると、暗号鍵・復号鍵を生成して当該鍵に鍵ＩＤを割り当て、生成した暗号鍵・復号鍵と当該鍵ＩＤとの組を前記鍵管理テーブルに保存し、当該暗号鍵とその鍵ＩＤとの組を有する鍵情

報応答メッセージを当該コンテンツサーバに返送する鍵管理サーバ内の鍵生成手段と、クライアントから鍵情報要求を受け取ると、当該鍵情報要求中の鍵ＩＤに対応する鍵を前記鍵管理テーブルから検索し、検索結果の復号鍵と鍵ＩＤとの組を有する鍵情報メッセージを当該クライアントに返送する鍵管理サーバ内の復号鍵送付手段と、暗号鍵とその鍵ＩＤとの組を保持するコンテンツサーバ内の暗号鍵テーブルと、鍵変更準備時点に達した時に、次に使用する暗号鍵を事前に取得するために鍵管理サーバに対して鍵作成要求を発行し、その応答として受信した鍵情報応答メッセージ中の暗号鍵と鍵ＩＤとの組を前記暗号鍵テーブルに保存するコンテンツサーバ内の暗号鍵取得手段と、前記暗号鍵取得手段により取得され前記暗号鍵テーブルに保持されている暗号鍵を用いて配信対象のデータの暗号化を行い、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットの送信を行うコンテンツサーバ内の暗号化・送信手段と、前記暗号鍵取得手段によって次に使用する暗号鍵の取得が行われた場合に、当該暗号鍵の鍵ＩＤを有する鍵変更予告メッセージのマルチキャスト配信を行うコンテンツサーバ内の鍵変更予告手段と、復号鍵とその鍵ＩＤとの組を保持するクライアント内の復号鍵テーブルと、鍵変更予告メッセージの受信時に、当該鍵変更予告メッセージ中の鍵ＩＤに対応する復号鍵を前記復号鍵テーブルから検索し、該当する復号鍵がない場合に鍵管理サーバに対して当該鍵ＩＤをキーにした鍵情報要求を送信し、その鍵情報要求の返信として鍵管理サーバから送信される鍵情報メッセージ中の復号鍵を取得し、当該復号鍵とその鍵ＩＤとの組を前記復号鍵テーブルに保存するクライアント内の復号鍵取得手段と、マルチキャストパケットを受信し、前記復号鍵取得手段により事前に取得され前記復号鍵管理テーブルに保持されており当該マルチキャストパケット中の鍵ＩＤに対応する復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行うクライアント内の受信・復号化手段とを有するように構成することも可能である。

【００１９】

ここで、本発明のマルチキャスト配信のための鍵管理方式は、上記の鍵管理サーバを、上記の鍵管理テーブル，鍵生成手段，および復号鍵送付手段として機能させるための鍵管理サーバ用鍵管理プログラムと、上記のコンテンツサーバを、上

記の暗号鍵テーブル，暗号鍵取得手段，暗号化・送信手段，および鍵変更予告手段として機能させるためのコンテンツサーバ用鍵管理プログラムと、上記のクライアントを、上記の復号鍵テーブル，復号鍵取得手段，および受信・復号化手段として機能させるためのクライアント用鍵管理プログラムとを有する態様で実現することも可能である。

【００２０】

なお、本発明のマルチキャスト配信のための鍵管理方式は、より一般的には、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、コンテンツサーバ群とクライアント群とからアクセス可能となるように配置されており、暗号鍵・復号鍵と当該鍵を一意に識別するための鍵ＩＤとの組を保持することによって鍵を管理する鍵管理サーバと、前記鍵管理サーバから暗号鍵とその鍵ＩＤとの組を受け取り、当該暗号鍵で暗号化されたデータと当該鍵ＩＤとを有するマルチキャストパケットをクライアント群に送信するコンテンツサーバと、前記コンテンツサーバからマルチキャストパケットを受信し、当該マルチキャストパケットに含まれる鍵ＩＤに対応する復号鍵を前記鍵管理サーバから取得し、当該復号鍵によって当該マルチキャストパケットに含まれる暗号化データの復号化を行うクライアントとを有すると表現することができる。

【００２１】

ここで、このマルチキャスト配信のための鍵管理方式に関しては、鍵管理サーバを鍵管理マスタサーバと複数の鍵管理スレーブサーバとに分けることによって、負荷分散を可能にすることもできる。また、コンテンツサーバが、使用する鍵を変更するときに、事前に鍵変更予告のマルチキャスト配信を行い、鍵管理サーバからの新たな復号鍵の取得をクライアントに促すことによって、鍵変更時にも遅延なく復号化を行うことを可能にすることもできる。

【００２２】

【発明の実施の形態】

次に、本発明について図面を参照して詳細に説明する。

【００２３】

（１）　第１の実施の形態

【００２４】

図１は、本発明の第１の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【００２５】

図１を参照すると、本実施の形態に係るマルチキャスト配信のための鍵管理方式は、マルチキャストパケットを送信するコンテンツサーバ１１，１２，…，１ｎ（ｎは正整数）と、マルチキャストパケットを受信するクライアント２１，２２，…，２ｍ（ｍは正整数）と、鍵（暗号鍵・復号鍵）の管理を行う鍵管理サーバ３１と、コンテンツサーバ１ｉ（ｉは１～ｎの正整数），クライアント２ｊ（ｊは１～ｍの正整数），および鍵管理サーバ３１を接続するネットワーク１００とを含んで構成されている。

【００２６】

コンテンツサーバ１ｉは、マルチキャストパケットで配信されるデータの暗号化に用いる鍵（暗号鍵）とその鍵を識別するための鍵ＩＤとの組を保存する暗号鍵テーブル１ｉ０を持つ。

【００２７】

また、各コンテンツサーバ１ｉは、暗号鍵取得手段１ｉ１と、暗号化・送信手段１ｉ２とを含んで構成されている。

【００２８】

クライアント２ｊは、マルチキャストパケットで配信される暗号化データの復号に用いる鍵（復号鍵）とその鍵を識別するための鍵ＩＤとの組を保存する復号鍵テーブル２ｊ０を持つ。

【００２９】

また、各クライアント２ｊは、復号鍵取得手段２ｊ１と、受信・復号化手段２ｊ２とを含んで構成されている。

【００３０】

鍵管理サーバ３１は、鍵（暗号鍵・復号鍵）とそれに対応する鍵ＩＤとの組を管理する鍵管理テーブル３１０を持つ。なお、一対の暗号化・復号化処理で用いられる暗号鍵と復号鍵とは、暗号化方式によって、同一の場合もあり異なる場合も

あるが、いずれにしても同一の鍵ＩＤによって識別される。

【００３１】

また、鍵管理サーバ３１は、鍵生成手段３１１と、復号鍵送付手段３１２とを含んで構成されている。

【００３２】

図２は、本実施の形態に係るマルチキャスト配信のための鍵管理方式の動作を説明するためのブロック図である。図２に示すように、コンテンツサーバ１ｉから鍵管理サーバ３１に鍵作成要求５１が送信され、その応答として、鍵管理サーバ３１からコンテンツサーバ１ｉに鍵情報応答メッセージ５２が送信される。また、クライアント２ｊから鍵管理サーバ３１に鍵情報要求６１が送信され、その応答として、鍵管理サーバ３１からクライアント２ｊに鍵情報メッセージ６２が送信される。

【００３３】

図３は、本実施の形態に係るマルチキャスト配信のための鍵管理方式における暗号化・送信処理を示す流れ図である。この処理は、暗号鍵有無判定ステップＡ１と、鍵作成要求発行ステップＡ２と、鍵生成ステップＡ３と、鍵ＩＤ割り当てステップＡ４と、鍵情報鍵管理テーブル保存ステップＡ５と、鍵情報応答メッセージ送信ステップＡ６と、鍵情報暗号鍵テーブル保存ステップＡ７と、データ暗号化ステップＡ８と、鍵ＩＤ保有マルチキャストパケット生成ステップＡ９と、マルチキャストパケット送信ステップＡ１０とからなる。

【００３４】

図４は、本実施の形態に係るマルチキャスト配信のための鍵管理方式における受信・復号化処理を示す流れ図である。この処理は、マルチキャストパケット受信ステップＢ１と、復号鍵有無判定ステップＢ２と、鍵情報要求発行ステップＢ３と、鍵管理テーブル検索ステップＢ４と、鍵情報メッセージ送信ステップＢ５と、鍵情報復号鍵テーブル保存ステップＢ６と、暗号化データ復号化ステップＢ７とからなる。

【００３５】

次に、図１～図４を参照して、上記のように構成された本実施の形態に係るマル

チキャスト配信のための鍵管理方式の全体の動作について詳細に説明する。

【００３６】

第１に、コンテンツサーバ側における暗号化・送信処理時の動作について説明する（図３参照）。

【００３７】

コンテンツサーバ１ｉ内の暗号化・送信手段１ｉ２は、配信対象のデータを暗号化してその暗号化データを有するマルチキャストパケットを送信する際に、その暗号化のための鍵（暗号鍵）が当該コンテンツサーバ１ｉの暗号鍵テーブル２ｉ０（自テーブル）に保持されているか否かを判定する（ステップＡ１）。

【００３８】

暗号化・送信手段１ｉ２は、ステップＡ１で「当該暗号鍵が自テーブルに保持されている」と判定した場合には、その暗号鍵を用いて配信対象のデータの暗号化を行い（ステップＡ８）、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットを生成し（ステップＡ９）、ネットワーク１００上への当該マルチキャストパケットの送信（マルチキャスト配信）を行う（ステップＡ１０）。

【００３９】

一方、暗号化・送信手段１ｉ２は、ステップＡ１で「当該暗号鍵が自テーブルに保持されていない」と判定した場合には、暗号鍵取得手段１ｉ１に制御を渡す。暗号鍵取得手段１ｉ１は、鍵管理サーバ３１に対して鍵作成要求５１（図２参照）を発行する（ステップＡ２）。

【００４０】

鍵作成要求５１を受け取った鍵管理サーバ３１内の鍵生成手段３１１は、要求された鍵（暗号鍵・復号鍵）を生成し（ステップＡ３）、その鍵に対して、鍵管理テーブル３１０内で一意に管理するための鍵ＩＤを割り当てる（ステップＡ４）。

【００４１】

さらに、鍵生成手段３１１は、ステップＡ３で生成した鍵とステップＡ４で割り当てた鍵ＩＤとの組を鍵管理テーブル３１０に保存し（ステップＡ５）、鍵作成

要求５１の発行元のコンテンツサーバ１ｉに対して当該鍵ＩＤと当該鍵（暗号鍵）との組を有する鍵情報応答メッセージ５２（図２参照）を送信する（ステップＡ６）。

【００４２】

鍵情報応答メッセージ５２を受信したコンテンツサーバ１ｉ内の暗号鍵取得手段１ｉ１は、受け取った鍵と鍵ＩＤとの組を自身の暗号鍵テーブル１ｉ０に保存する（ステップＡ７）。

【００４３】

さらに、当該コンテンツサーバ１ｉ内の暗号化・送信手段１ｉ２は、鍵管理サーバ３１から受け取った暗号鍵を用いて配信対象のデータの暗号化を行い（ステップＡ８）、その暗号化データと当該暗号鍵に対応する鍵ＩＤとを有するマルチキャストパケットを生成し（ステップＡ９）、ネットワーク１００上への当該マルチキャストパケットの送信（マルチキャスト配信）を行う（ステップＡ１０）。

【００４４】

なお、図２に示すコンテンツサーバ１２のように、暗号鍵テーブル（図２では暗号鍵テーブル１２０）内に複数の鍵が保持されている場合には、マルチキャスト配信の対象となるデータの内容や時刻によって当該複数の鍵を使い分けることも可能である。すなわち、本実施の形態に限らず、本発明では、コンテンツサーバ側で、複数の暗号鍵と鍵ＩＤとの組を同時に保持しておき、マルチキャスト配信において使用する暗号鍵を適時変更することも可能である。

【００４５】

第２に、クライアント側における受信・復号化処理時の動作について説明する（図４参照）。

【００４６】

クライアント２ｊ内の受信・復号化手段２ｊ２は、コンテンツサーバ１ｉから配信されたマルチキャストパケットを受信すると（ステップＢ１）、当該マルチキャストパケットに含まれる鍵ＩＤを参照し、当該鍵ＩＤに対応する鍵（復号鍵）が自身の復号鍵テーブル８ｊ（自テーブル）にあるか否かを判定（検索）する（ステップＢ２）。

【００４７】

受信・復号化手段２ｊ２は、ステップＢ２の検索で「当該鍵ＩＤに対応する復号鍵がある」と判定した場合には、その復号鍵を用いて当該マルチキャストパケット中の暗号化データの復号化を行う（ステップＢ７）。

【００４８】

一方、受信・復号化手段２ｊ２は、ステップＢ２の検索で「当該鍵ＩＤに対応する復号鍵がない」と判定した場合には、復号鍵取得手段２ｊ１に制御を渡す。復号鍵取得手段２ｊ１は、当該マルチキャストパケットに含まれる鍵ＩＤを使って（当該鍵ＩＤをキーにして）、鍵情報要求６１（図２参照）を鍵管理サーバ３１に発行する（ステップＢ３）。すなわち、当該鍵ＩＤに対応する復号鍵に関する鍵情報（鍵ＩＤと復号鍵との組）を、鍵管理サーバ３１に対して要求する。

【００４９】

その鍵情報要求６１を受け取った鍵管理サーバ３１内の復号鍵送付手段３１２は、鍵情報要求６１中の鍵ＩＤを用いて鍵管理テーブル３１０の検索を行い、当該鍵ＩＤに対応する鍵を取得する（ステップＢ４）。

【００５０】

その上で、復号鍵送付手段３１２は、鍵管理テーブル３１０から取得した鍵（復号鍵）とその鍵ＩＤとの組を有する鍵情報メッセージ６２（図２参照）を、鍵情報要求６１に対する返信として、鍵情報要求６１を発行したクライアント２ｊに送信する（ステップＢ５）。

【００５１】

当該クライアント２ｊ内の復号鍵取得手段２ｊ１は、当該鍵情報メッセージ６２を鍵管理サーバ３１から受け取ると、以降のマルチキャストパケット受信時の復号化処理の際に用いるために、当該鍵情報メッセージ６２中の復号鍵と鍵ＩＤとの組を自身の復号鍵テーブル２ｊ０に保存しておく（ステップＢ６）。

【００５２】

さらに、当該クライアント２ｊ内の受信・復号化手段２ｊ２は、その復号鍵を用いて、ステップＢ１で受信したマルチキャストパケット中の暗号化データの復号化を行う（ステップＢ７）。

【００５３】

なお、クライアント２ｊの復号鍵テーブル２ｊ０は、初期状態では１つの鍵情報（鍵ＩＤと鍵との組）も持っていない。また、復号鍵テーブル２ｊ０中の鍵とその鍵ＩＤとの組は、一定時間用いられないと、復号鍵テーブル２ｊ０から消去される。

【００５４】

（２）　第２の実施の形態

【００５５】

図５は、本発明の第２の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【００５６】

図５を参照すると、本実施の形態に係るマルチキャスト配信のための鍵管理方式は、マルチキャストパケットを送信するコンテンツサーバ１１，１２，…，１ｎ（ｎは正整数）と、マルチキャストパケットを受信するクライアント２１，２２，…，２ｍ（ｍは正整数）と、鍵（暗号鍵・復号鍵）の管理を行う鍵管理マスタ（ＭＡＳＴＥＲ）サーバ４０および鍵管理スレーブ（ＳＬＡＶＥ）サーバ４１，…，４ｐ（ｐは正整数）と、コンテンツサーバ１ｉ（ｉは１～ｎの正整数），クライアント２ｊ（ｊは１～ｍの正整数），鍵管理マスタサーバ４０，および鍵管理スレーブサーバ４ｋ（ｋは１～ｐの正整数）を接続するネットワーク１００とを含んで構成されている。

【００５７】

本実施の形態（第２の実施の形態）と第１の実施の形態とを比較すると、第１の実施の形態（図１参照）における鍵管理サーバ３１に対応するものとして、本実施の形態では、鍵管理マスタサーバ４０と複数の鍵管理スレーブサーバ４ｋとが分かれて存在している点が異なっている。

【００５８】

すなわち、図５に示す本実施の形態の構成は、鍵管理サーバを鍵管理マスタサーバ４０と鍵管理スレーブサーバ４ｋとに分けて、鍵管理スレーブサーバ４ｋを複数用意することによって、鍵管理サーバの負荷の分散を可能にしている。

【００５９】

なお、鍵管理マスタサーバ４０は、鍵管理テーブル４００を有しており、鍵生成・配布手段４０１を含んで構成されている。

【００６０】

また、鍵管理スレーブサーバ４ｋは、鍵管理テーブル４ｋ０を有しており、鍵保存手段４ｋ１と、復号鍵送付手段４ｋ２とを含んで構成されている。

【００６１】

図６は、本実施の形態に係るマルチキャスト配信のための鍵管理方式の動作を説明するためのブロック図である。図６に示すように、コンテンツサーバ１ｉ（図６では、簡単化のためにコンテンツサーバ１１のみを示している）から鍵管理マスタサーバ４０に鍵作成要求５１が送信され、その応答として、鍵管理マスタサーバ４０からコンテンツサーバ１ｉに鍵情報応答メッセージ５２が送信される。このときに、鍵管理マスタサーバ４０から鍵管理スレーブサーバ４１～４ｐに鍵情報配布メッセージ７１～７ｐが送信される。また、クライアント２ｊから鍵管理スレーブサーバ４１～４ｐのいずれかに鍵情報要求６１が送信され、その応答として、当該鍵管理スレーブサーバ４ｋからクライアント２ｊに鍵情報メッセージ６２が送信される。

【００６２】

次に、図５および図６を参照して（図１～図４も適宜参照する）、上記のように構成された本実施の形態に係るマルチキャスト配信のための鍵管理方式の動作について、第１の実施の形態とは異なる点を中心にして説明する。

【００６３】

第１に、暗号化・送信処理時の動作について説明する。

【００６４】

第１の実施の形態では、コンテンツサーバ１ｉは、図３中のステップＡ１で「暗号鍵が自テーブルに保持されていない」と判定した場合に、ステップＡ２で、鍵管理サーバ３１に鍵作成要求５１（図２参照）を発行していた。

【００６５】

これに対して、本実施の形態では、コンテンツサーバ１ｉ（コンテンツサーバｉ

１内の暗号鍵取得手段１ｉ１）は、鍵管理マスタサーバ４０に対して、鍵作成要求５１（図６参照）を発行する。

【００６６】

そして、鍵作成要求５１を受け取った鍵管理マスタサーバ４０内の鍵生成・配布手段４０１は、鍵（暗号鍵・復号鍵）を生成し、その鍵に対して、鍵管理テーブル４００内で一意に管理するための鍵ＩＤを割り当てる。

【００６７】

また、鍵生成・配布手段４０１は、生成した鍵とその鍵に割り当てた鍵ＩＤとの組を鍵管理テーブル４００に保存し、鍵作成要求５１に対する応答として、当該コンテンツサーバ１ｉに対して当該鍵ＩＤと当該鍵（暗号鍵）との組を有する鍵情報応答メッセージ５２（図６参照）を送信する。

【００６８】

さらに、鍵管理マスタサーバ４０内の鍵生成・配布手段４０１は、この鍵と鍵ＩＤとの組を有する鍵情報配布メッセージ７１～７ｐ（図６参照）を、全ての鍵管理スレーブサーバ４１～４ｐに対しても送る。

【００６９】

各鍵管理スレーブサーバ４ｋ内の鍵保存手段４ｋ１は、当該鍵と当該鍵ＩＤとの組を、自己の鍵管理テーブル４ｋ０に保存する。

【００７０】

第２に、受信・復号化処理時の動作について説明する。

【００７１】

第１の実施の形態では、クライアント２ｊは、図４中のステップＢ２の検索（判定）で「マルチキャストパケット中の鍵ＩＤに対応する復号鍵が自テーブルにない」と判定した場合には、ステップＢ３で、コンテンツサーバ１ｉから受け取ったマルチキャストパケットに含まれている鍵ＩＤを使って、鍵情報要求６１（図２参照）を鍵管理サーバ３１に発行していた。

【００７２】

これに対して、本実施の形態では、クライアント２ｊは、鍵情報要求６１（図６参照）を発行する時に、複数の鍵管理スレーブサーバ４１～４ｐのいずれかにそ

の鍵情報要求６１を送る。このとき、どの鍵管理スレーブサーバ４ｋに送るかを決める方法としては、例えば、以下のａおよびｂに示す２つの方法がある。

【００７３】

ａ．各クライアント２ｊ毎に、どの鍵管理スレーブサーバ４ｋに鍵情報要求６１を送るかを事前に決めておく方法

【００７４】

ｂ．クライアント２ｊが鍵情報要求６１を送る１回毎に、送り先の鍵管理スレーブサーバ４ｋを変える方法（ラウンドロビン法）

【００７５】

その鍵情報要求６１を受け取った鍵管理スレーブサーバ４ｋ内の復号鍵送付手段４ｋ２は、鍵情報要求６１中の鍵ＩＤを用いて自己の鍵管理テーブル４ｋ０の検索を行い、当該鍵ＩＤに対応する鍵を取得し、取得した鍵（復号鍵）とその鍵ＩＤとの組を有する鍵情報メッセージ６２（図６参照）を、鍵情報要求６１に対する返信として、鍵情報要求６１を発行したクライアント２ｊに送信する。

【００７６】

なお、上記以外の動作に関しては、本実施の形態に係るマルチキャスト配信のための鍵管理方式は、第１の実施の形態と同様の動作（処理）を行う（図３および図４参照）。

【００７７】

このように、本実施の形態では、クライアント２ｊからの鍵情報要求６１を受ける鍵管理スレーブサーバ４ｋが複数用意されているため、前述の第１の実施の形態と比べて、鍵管理サーバの負荷を分散することができる。

【００７８】

（３）　第３の実施の形態

【００７９】

図７は、本発明の第３の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【００８０】

図７を参照すると、本実施の形態に係るマルチキャスト配信のための鍵管理方式

は、図１に示す第１の実施の形態と同様に、マルチキャストパケットを送信するコンテンツサーバ１１，１２，…，１ｎ（ｎは正整数）と、マルチキャストパケットを受信するクライアント２１，２２，…，２ｍ（ｍは正整数）と、鍵（暗号鍵・復号鍵）の管理を行う鍵管理サーバ３１と、コンテンツサーバ１ｉ（ｉは１～ｎの正整数），クライアント２ｊ（ｊは１～ｍの正整数），および鍵管理サーバ３１を接続するネットワーク１００とを含んで構成されている。ただし、本実施の形態におけるコンテンツサーバ１ｉは、本実施の形態に特有の構成要素として、鍵変更予告手段１ｉ３を有している。

【００８１】

本実施の形態（第３の実施の形態）と第１の実施の形態とを比較すると、本実施の形態の基本的な構成は第１の実施の形態（図１参照）と同じであるが、コンテンツサーバ１ｉが暗号化に用いる鍵を変更する前に、事前にクライアント２ｊに対して鍵変更予告として、新たに用いる予定の鍵の鍵ＩＤを通知し、クライアント２ｊ側で新たな鍵情報（復号鍵と鍵ＩＤとの組）を事前に鍵管理サーバ３１から取得しておく点が異なっている。

【００８２】

このような特有の構成・動作によって、コンテンツサーバ１ｉ側で暗号鍵が変わった時に、クライアント２ｊ側で遅延なく変更後の鍵による暗号化データの復号化が可能になるという特有の効果が生じる。

【００８３】

図８は、本実施の形態に係るマルチキャスト配信のための鍵管理方式の具体的な動作を説明するためのシーケンス図である。

【００８４】

図９は、本実施の形態に係るマルチキャスト配信のための鍵管理方式における鍵変更予告関連処理を示す流れ図である。この処理は、鍵変更準備時点到達認識ステップＣ１と、鍵作成要求発行ステップＣ２と、鍵生成ステップＣ３と、鍵ＩＤ割り当てステップＣ４と、鍵情報鍵管理テーブル保存ステップＣ５と、鍵情報応答メッセージ送信ステップＣ６と、鍵情報暗号鍵テーブル保存ステップＣ７と、鍵変更予告メッセージマルチキャスト配信ステップＣ８と、復号鍵有無判定ステ

ップＣ９と、鍵情報要求発行ステップＣ１０と、鍵管理テーブル検索ステップＣ１１と、鍵情報メッセージ送信ステップＣ１２と、鍵情報復号鍵テーブル保存ステップＣ１３とからなる。

【００８５】

次に、図７～図９を参照して（図１～図４も適宜参照する）、上記のように構成された本実施の形態に係るマルチキャスト配信のための鍵管理方式の動作について、第１の実施の形態とは異なる点を中心にして説明する。

【００８６】

図８に示すように、クライアント２ｊ（図８では、代表としてクライアント２１を示している）は、コンテンツサーバ１ｉ（図８では、代表としてコンテンツサーバ１１を示している）から、鍵ＩＤと暗号化データとを有するマルチキャストパケットを受信し、その鍵ＩＤに対応する鍵（復号鍵）で当該暗号化データの復号化を行っている。このような動作は、前述の第１の実施の形態における動作と同様である。

【００８７】

ここで、図８に示す動作シーケンスでは、期間Ａにおいては、鍵ＩＤ１を有するマルチキャストパケット９１（鍵ＩＤ１で識別される暗号鍵で暗号化されたデータを有するマルチキャストパケット）が送受信されており、期間Ｂにおいては、鍵ＩＤ２を有するマルチキャストパケット９２（鍵ＩＤ２で識別される暗号鍵で暗号化されたデータを有するマルチキャストパケット）が送受信されているものとする。

【００８８】

上記のようなマルチキャストパケットの配信が行われていることを前提として、本実施の形態では、以下のような鍵変更予告関連処理が行われる（図９参照）。

【００８９】

コンテンツサーバ１ｉ内の暗号鍵取得手段１ｉ１は、ある時点（実際に新たな鍵を使用する時点よりも前の時点の任意的な時点。「鍵変更準備時点」と呼ぶ）に達したことを認識すると（ステップＣ１）、新たな鍵を得るために、鍵作成要求５１を鍵管理サーバ３１に送る（ステップＣ２）。

【００９０】

図８の例では、コンテンツサーバ１１は、鍵変更準備時点ａにおいて、鍵管理サーバ３１に鍵作成要求５１を送信する。

【００９１】

鍵管理サーバ３１内の鍵生成手段３１１は、鍵作成要求５１で要求された鍵（暗号鍵および復号鍵）を生成し（ステップＣ３）、その鍵に鍵ＩＤを割り当て（ステップＣ４）、その鍵ＩＤとその鍵との組を鍵管理テーブル３１０に保存し（ステップＣ５）、その鍵ＩＤとその鍵（暗号鍵）との組を有する鍵情報応答メッセージ５２を鍵作成要求５１の発行元のコンテンツサーバ１ｉに送信する（ステップＣ６）。

【００９２】

図８の例では、鍵管理サーバ３１は、鍵２を生成し、その鍵２に鍵ＩＤ２を割り当て、鍵ＩＤ２と鍵２との組を有する鍵情報応答メッセージ５２をコンテンツサーバ１１に送信する。

【００９３】

鍵情報応答メッセージ５２を受信したコンテンツサーバ１ｉ内の暗号鍵取得手段１ｉ１は、新たな鍵の鍵情報（受け取った鍵と鍵ＩＤとの組）を自身の暗号鍵テーブル１ｉ０に保存する（ステップＣ７）。

【００９４】

さらに、コンテンツサーバ１ｉ内の鍵変更予告手段１ｉ３は、新たな鍵ＩＤと鍵との組を取得した段階で、変更後の鍵ＩＤと鍵変更予告とを有する鍵変更予告メッセージ８１のマルチキャスト配信を行う（ステップＣ８）。

【００９５】

図８の例では、コンテンツサーバ１１は、鍵変更予告と鍵ＩＤ２とを有する鍵変更予告メッセージ８１のマルチキャスト配信を行う。

【００９６】

鍵変更予告メッセージ８１を受信した各クライアント２ｊ内の復号鍵取得手段２ｊ１は、当該鍵変更予告メッセージ８１に含まれている鍵ＩＤによって自身の復号鍵テーブル２ｊ０の検索を行い、当該鍵ＩＤに対応する鍵（復号鍵）が自身の

復号鍵テーブル２ｊ０（自テーブル）にあるか否かを判定する（ステップＣ９）。

【００９７】

復号鍵取得手段２ｊ１は、ステップＣ９の検索で「当該鍵ＩＤに対応する復号鍵がない」と判定した場合には、当該鍵変更予告メッセージ８１に含まれる鍵ＩＤを使って、鍵情報要求６１を鍵管理サーバ３１に発行する（ステップＣ１０）。すなわち、当該鍵ＩＤに対応する復号鍵に関する鍵情報を、鍵管理サーバ３１に対して要求する。なお、ステップＣ９の検索で「当該鍵ＩＤに対応する復号鍵がある」と判定した場合には、ステップＣ１０以降の処理は不要となるので、処理を終了する。

【００９８】

図８の例では、クライアント２１は、鍵変更予告メッセージ８１に含まれている鍵ＩＤ２に対応する鍵（復号鍵）を取得するために、鍵ＩＤ２を有する鍵情報要求を鍵管理サーバ３１に発行する。

【００９９】

その鍵情報要求６１を受け取った鍵管理サーバ３１内の復号鍵送付手段３１２は、鍵情報要求６１中の鍵ＩＤを用いて鍵管理テーブル３１０の検索を行い、当該鍵ＩＤに対応する鍵を取得する（ステップＣ１１）。

【０１００】

その上で、復号鍵送付手段３１２は、鍵管理テーブル３１０から取得した鍵（復号鍵）とその鍵ＩＤとの組を有する鍵情報メッセージ６２を、鍵情報要求６１に対する返信として、鍵情報要求６１を発行したクライアント２ｊに送信する（ステップＣ１２）。

【０１０１】

当該クライアント２ｊ内の復号鍵取得手段２ｊ１は、当該鍵情報メッセージ６２を鍵管理サーバ３１から受け取ると、次の期間（例えば、図８中の期間Ａに対する期間Ｂ）におけるマルチキャストパケット受信時の復号化処理の際に用いるために、当該鍵情報メッセージ６２中の復号鍵と鍵ＩＤとの組を自身の復号鍵テーブル２ｊ０に保存しておく（ステップＣ１３）。

【０１０２】

図８の例では、鍵管理サーバ３１は、鍵ＩＤ２と鍵２との組を有する鍵情報メッセージ６２をクライアント２１に返信し、クライアント２１は、その鍵（復号鍵）２と鍵ＩＤ２との組を自身の復号鍵テーブル２１０に保存する。

【０１０３】

その後（期間Ｂにおいて）、コンテンツサーバ１１は、配信対象のデータの暗号化に鍵（暗号鍵）２を用い、鍵２で暗号化したデータと鍵ＩＤ２とを有するマルチキャストパケット９２を送信する。

【０１０４】

このマルチキャストパケット９２を受信したクライアント２１は、鍵管理テーブル２１０内に保持している鍵ＩＤ２に対応する鍵（復号鍵）２を用いて、即座に暗号化データの復号化を行うことが可能になる。

【０１０５】

なお、上記以外の動作に関しては、本実施の形態においても、第１の実施の形態と同様の動作（処理）が行われる。ただし、図３および図４に示す一連の処理において、あらかじめ暗号鍵および復号鍵の取得が行われているので、上記の変更予告関連処理が正常に行われている限り、図３中のステップＡ２～Ａ７の処理および図４中のステップＢ３～Ｂ６の処理が行われることはない。

【０１０６】

前述の第１の実施の形態では、クライアント２ｊは、鍵が変わった時に受信したマルチキャストパケットに含まれる鍵ＩＤを見てはじめて鍵が変わったことを知ることになる。このため、クライアント２ｊは、多くの場合に、その時点で鍵管理サーバ３１に新たな鍵の送付を要求し、その応答によって新たな鍵を取得することになる。このような場合に、クライアント２ｊは、その応答を受け取るまで、新たな鍵ＩＤを有するマルチキャストパケット中の暗号化データの復号化ができない。

【０１０７】

これに対して、本実施の形態（第３の実施の形態）では、実際に鍵を変更する前に、コンテンツサーバ１ｉがクライアント２ｊに鍵変更予告を出しておき、あら

かじめクライアント２ｊに新たに用いる鍵を取得させておくことによって、鍵変更時に遅延なく新たな鍵による暗号化データの復号化を行うことが可能となっている。

【０１０８】

（４）　第４の実施の形態

【０１０９】

図１０は、本発明の第４の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【０１１０】

図１０を参照すると、本発明の第４の実施の形態に係るマルチキャスト配信のための鍵管理方式は、図１に示した第１の実施の形態に係るマルチキャスト配信のための鍵管理方式に対して、コンテンツサーバ用鍵管理プログラム１００１，クライアント用鍵管理プログラム１００２，および鍵管理サーバ用鍵管理プログラム１００３を備える点が異なっている。

【０１１１】

コンテンツサーバ用鍵管理プログラム１００１は、コンテンツサーバ１ｉに読み込まれ、当該コンテンツサーバ１ｉの動作を暗号鍵テーブル１ｉ０，暗号鍵取得手段１ｉ１，および暗号化・送信手段１ｉ２として制御する。コンテンツサーバ用鍵管理プログラム１００１の制御によるコンテンツサーバ１ｉの動作（暗号鍵テーブル１ｉ０，暗号鍵取得手段１ｉ１，および暗号化・送信手段１ｉ２に関する動作）は、第１の実施の形態におけるコンテンツサーバ１ｉの動作と全く同様になるので、その詳しい説明を割愛する。

【０１１２】

また、クライアント用鍵管理プログラム１００２は、クライアント２ｊに読み込まれ、当該クライアント２ｊの動作を復号鍵テーブル２ｊ０，復号鍵取得手段２ｊ１，および受信・復号化手段２ｊ２として制御する。クライアント用鍵管理プログラム１００２の制御によるクライアント２ｊの動作（復号鍵テーブル２ｊ０，復号鍵取得手段２ｊ１，および受信・復号化手段２ｊ２に関する動作）は、第１の実施の形態におけるクライアント２ｊの動作と全く同様になるので、その詳

しい説明を割愛する。

【０１１３】

さらに、鍵管理サーバ用鍵管理プログラム１００３は、鍵管理サーバ３１に読み込まれ、当該鍵管理サーバ３１の動作を鍵管理テーブル３１０，鍵生成手段３１１，および復号鍵送付手段３１２として制御する。鍵管理サーバ用鍵管理プログラム１００３の制御による鍵管理サーバ３１の動作（鍵管理テーブル３１０，鍵生成手段３１１，および復号鍵送付手段３１２に関する動作）は、第１の実施の形態における鍵管理サーバ３１の動作と全く同様になるので、その詳しい説明を割愛する。

【０１１４】

（５）　第５の実施の形態

【０１１５】

図１１は、本発明の第５の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【０１１６】

図１１を参照すると、本発明の第５の実施の形態に係るマルチキャスト配信のための鍵管理方式は、図５に示した第２の実施の形態に係るマルチキャスト配信のための鍵管理方式に対して、コンテンツサーバ用鍵管理プログラム１１０１，クライアント用鍵管理プログラム１１０２，鍵管理マスタサーバ用鍵管理プログラム１１０３，および鍵管理スレーブサーバ用鍵管理プログラム１１０４を備える点が異なっている。

【０１１７】

コンテンツサーバ用鍵管理プログラム１１０１は、コンテンツサーバ１ｉに読み込まれ、当該コンテンツサーバ１ｉの動作を暗号鍵テーブル１ｉ０，暗号鍵取得手段１ｉ１，および暗号化・送信手段１ｉ２として制御する。コンテンツサーバ用鍵管理プログラム１１０１の制御によるコンテンツサーバ１ｉの動作（暗号鍵テーブル１ｉ０，暗号鍵取得手段１ｉ１，および暗号化・送信手段１ｉ２に関する動作）は、第２の実施の形態におけるコンテンツサーバ１ｉの動作と全く同様になるので、その詳しい説明を割愛する。

【０１１８】

また、クライアント用鍵管理プログラム１１０２は、クライアント２ｊに読み込まれ、当該クライアント２ｊの動作を復号鍵テーブル２ｊ０，復号鍵取得手段２ｊ１，および受信・復号化手段２ｊ２として制御する。クライアント用鍵管理プログラム１１０２の制御によるクライアント２ｊの動作（復号鍵テーブル２ｊ０，復号鍵取得手段２ｊ１，および受信・復号化手段２ｊ２に関する動作）は、第２の実施の形態におけるクライアント２ｊの動作と全く同様になるので、その詳しい説明を割愛する。

【０１１９】

さらに、鍵管理マスタサーバ用鍵管理プログラム１１０３は、鍵管理マスタサーバ４０に読み込まれ、当該鍵管理マスタサーバ４０の動作を鍵管理テーブル４００および鍵生成・配布手段４０１として制御する。鍵管理マスタサーバ用鍵管理プログラム１１０３の制御による鍵管理マスタサーバ４０の動作（鍵管理テーブル４００および鍵生成・配布手段４０１に関する動作）は、第２の実施の形態における鍵管理マスタサーバ４０の動作と全く同様になるので、その詳しい説明を割愛する。

【０１２０】

加えて、鍵管理スレーブサーバ用鍵管理プログラム１１０４は、鍵管理スレーブサーバ４ｋに読み込まれ、当該鍵管理スレーブサーバ４ｋの動作を鍵管理テーブル４ｋ０，鍵保存手段４ｋ１，および復号鍵送付手段４ｋ２として制御する。鍵管理スレーブサーバ用鍵管理プログラム１１０４の制御による鍵管理スレーブサーバ４ｋの動作（鍵管理テーブル４ｋ０，鍵保存手段４ｋ１，および復号鍵送付手段４ｋ２に関する動作）は、第２の実施の形態における鍵管理スレーブサーバ４ｋの動作と全く同様になるので、その詳しい説明を割愛する。

【０１２１】

（６）　第６の実施の形態

【０１２２】

図１２は、本発明の第６の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【０１２３】

図１２を参照すると、本発明の第６の実施の形態に係るマルチキャスト配信のための鍵管理方式は、図７に示した第３の実施の形態に係るマルチキャスト配信のための鍵管理方式に対して、コンテンツサーバ用鍵管理プログラム１２０１，クライアント用鍵管理プログラム１２０２，および鍵管理サーバ用鍵管理プログラム１２０３を備える点が異なっている。

【０１２４】

コンテンツサーバ用鍵管理プログラム１２０１は、コンテンツサーバ１ｉに読み込まれ、当該コンテンツサーバ１ｉの動作を暗号鍵テーブル１ｉ０，暗号鍵取得手段１ｉ１，暗号化・送信手段１ｉ２，および鍵変更予告手段１ｉ３として制御する。コンテンツサーバ用鍵管理プログラム１２０１の制御によるコンテンツサーバ１ｉの動作（暗号鍵テーブル１ｉ０，暗号鍵取得手段１ｉ１，暗号化・送信手段１ｉ２，および鍵変更予告手段１ｉ３に関する動作）は、第３の実施の形態におけるコンテンツサーバ１ｉの動作と全く同様になるので、その詳しい説明を割愛する。

【０１２５】

また、クライアント用鍵管理プログラム１２０２は、クライアント２ｊに読み込まれ、当該クライアント２ｊの動作を復号鍵テーブル２ｊ０，復号鍵取得手段２ｊ１，および受信・復号化手段２ｊ２として制御する。クライアント用鍵管理プログラム１２０２の制御によるクライアント２ｊの動作（復号鍵テーブル２ｊ０，復号鍵取得手段２ｊ１，および受信・復号化手段２ｊ２に関する動作）は、第３の実施の形態におけるクライアント２ｊの動作と全く同様になるので、その詳しい説明を割愛する。

【０１２６】

さらに、鍵管理サーバ用鍵管理プログラム１２０３は、鍵管理サーバ３１に読み込まれ、当該鍵管理サーバ３１の動作を鍵管理テーブル３１０，鍵生成手段３１１，および復号鍵送付手段３１２として制御する。鍵管理サーバ用鍵管理プログラム１２０３の制御による鍵管理サーバ３１の動作（鍵管理テーブル３１０，鍵生成手段３１１，および復号鍵送付手段３１２に関する動作）は、第３の実施の

形態における鍵管理サーバ３１の動作と全く同様になるので、その詳しい説明を割愛する。

【０１２７】

【発明の効果】

以上説明したように、本発明によると、暗号化データのマルチキャスト配信が行われるネットワークシステムにおいて、複数のマルチキャスト配信の各配信対象データが別々の鍵によって暗号化されている場合に、異なるそれぞれの鍵（暗号鍵・復号鍵）の管理を容易に実現することができるという効果が生じる。

【０１２８】

このような効果が生じる理由は、コンテンツサーバが暗号化処理で使用する鍵を区別する鍵ＩＤを、暗号化データを有するマルチキャストパケットに含めてクライアントに送り、クライアント側ではその鍵ＩＤによってコンテンツサーバ側で暗号化に用いている鍵が変わったことを知ることができるため、暗号化に用いる鍵が変わった場合にも、クライアント側から鍵管理サーバ側に対して必要に応じて新たな復号鍵を要求することができるので、鍵管理サーバ側やコンテンツサーバ側でクライアントに関する情報の管理を行う必要がなくなるからである。

【図面の簡単な説明】

【図１】

本発明の第１の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【図２】

図１に示すマルチキャスト配信のための鍵管理方式の動作を説明するためのブロック図である。

【図３】

図１に示すマルチキャスト配信のための鍵管理方式の暗号化・送信処理を示す流れ図である。

【図４】

図１に示すマルチキャスト配信のための鍵管理方式の受信・復号化処理を示す流れ図である。

【図５】

本発明の第２の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【図６】

図５に示すマルチキャスト配信のための鍵管理方式の動作を説明するためのブロック図である。

【図７】

本発明の第３の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【図８】

図７に示すマルチキャスト配信のための鍵管理方式の鍵変更予告関連処理を示す流れ図である。

【図９】

図７に示すマルチキャスト配信のための鍵管理方式の具体的な動作を説明するためのシーケンス図である。

【図１０】

本発明の第４の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【図１１】

本発明の第５の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【図１２】

本発明の第６の実施の形態に係るマルチキャスト配信のための鍵管理方式の構成を示すブロック図である。

【符号の説明】

１１，１２，…，１ｎ　コンテンツサーバ

２１，２２，…，２ｍ　クライアント

３１　鍵管理サーバ

４０　鍵管理マスタサーバ

４１，…，４ｐ　鍵管理スレーブサーバ

５１　鍵作成要求

５２　鍵情報応答メッセージ

６１　鍵情報要求

６２　鍵情報メッセージ

７１，…，７ｐ　鍵情報配布メッセージ

８１　鍵変更予告メッセージ

９１，９２　マルチキャストパケット

１００　ネットワーク

１１０，１２０，…，１ｎ０　暗号鍵テーブル

１１１，１２１，…，１ｎ１　暗号鍵取得手段

１１２，１２２，…，１ｎ２　暗号化・送信手段

１１３，１２３，…，１ｎ３　鍵変更予告手段

２１０，２２０，…，２ｍ０　復号鍵テーブル

２１１，２２１，…，２ｍ１　復号鍵取得手段

２１２，２２２，…，２ｍ２　受信・復号化手段

３１０，４００，４１０，…，４ｐ０　鍵管理テーブル

３１１　鍵生成手段

３１２，４１２，…，４ｐ２　復号鍵送付手段

４０１　鍵生成・配布手段

４１１，…，４ｐ１　鍵保存手段

１００１，１１０１，１２０１　コンテンツサーバ用鍵管理プログラム

１００２，１１０２，１２０２　クライアント用鍵管理プログラム

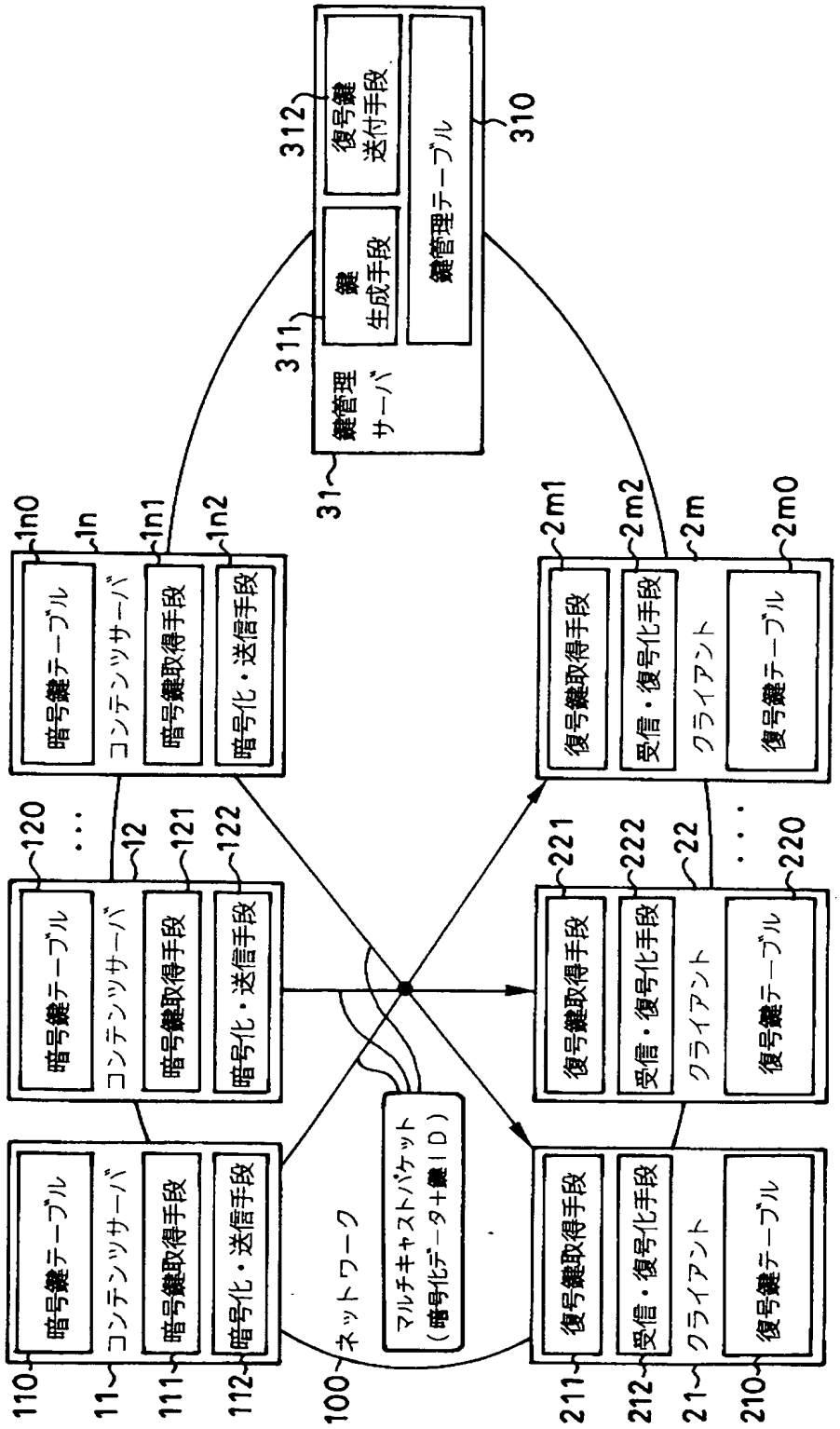
１００３，１２０３　鍵管理サーバ用鍵管理プログラム

１１０３　鍵管理マスタサーバ用鍵管理プログラム

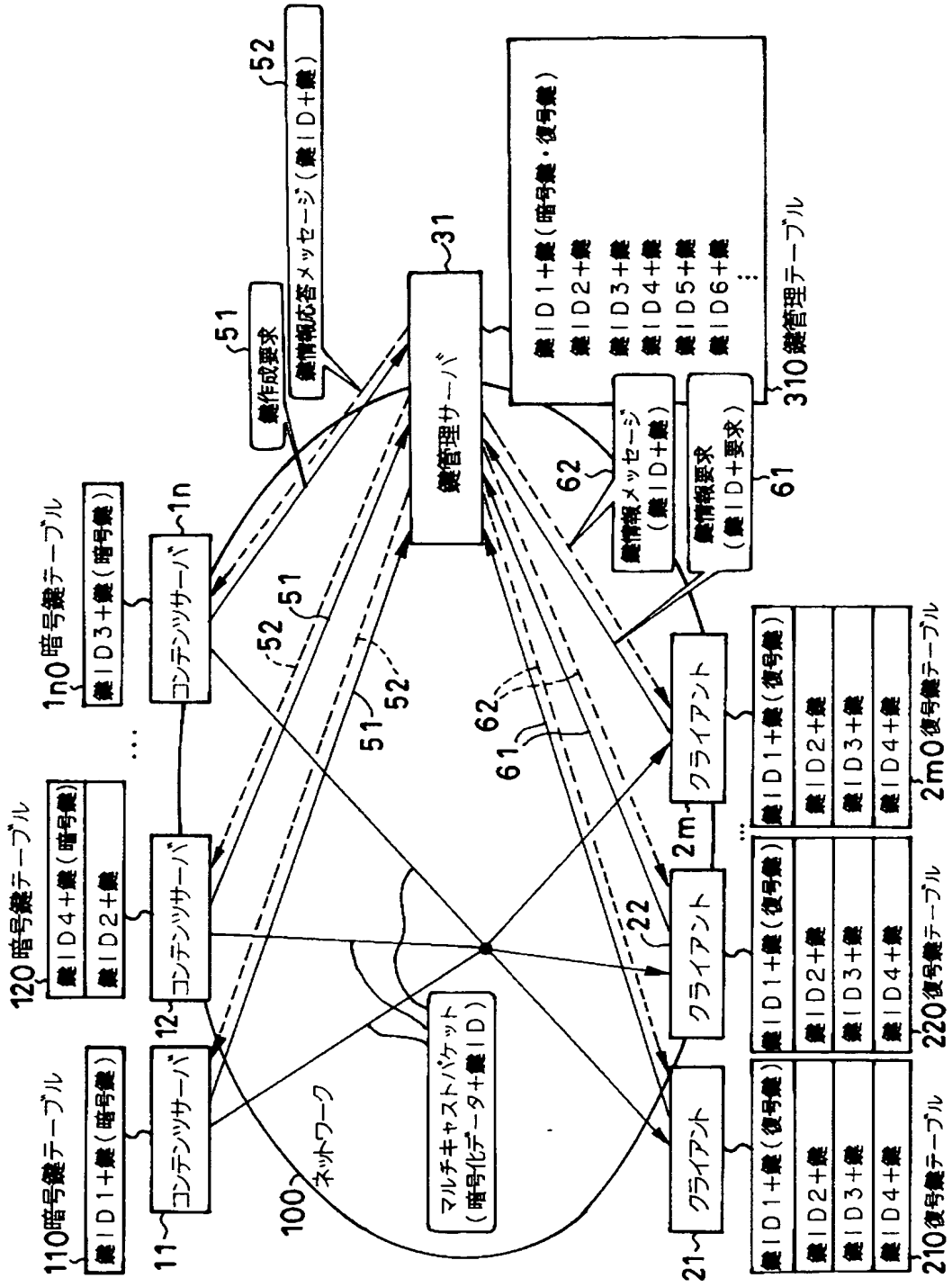
１１０４　鍵管理スレーブサーバ用鍵管理プログラム

【書類名】　図面

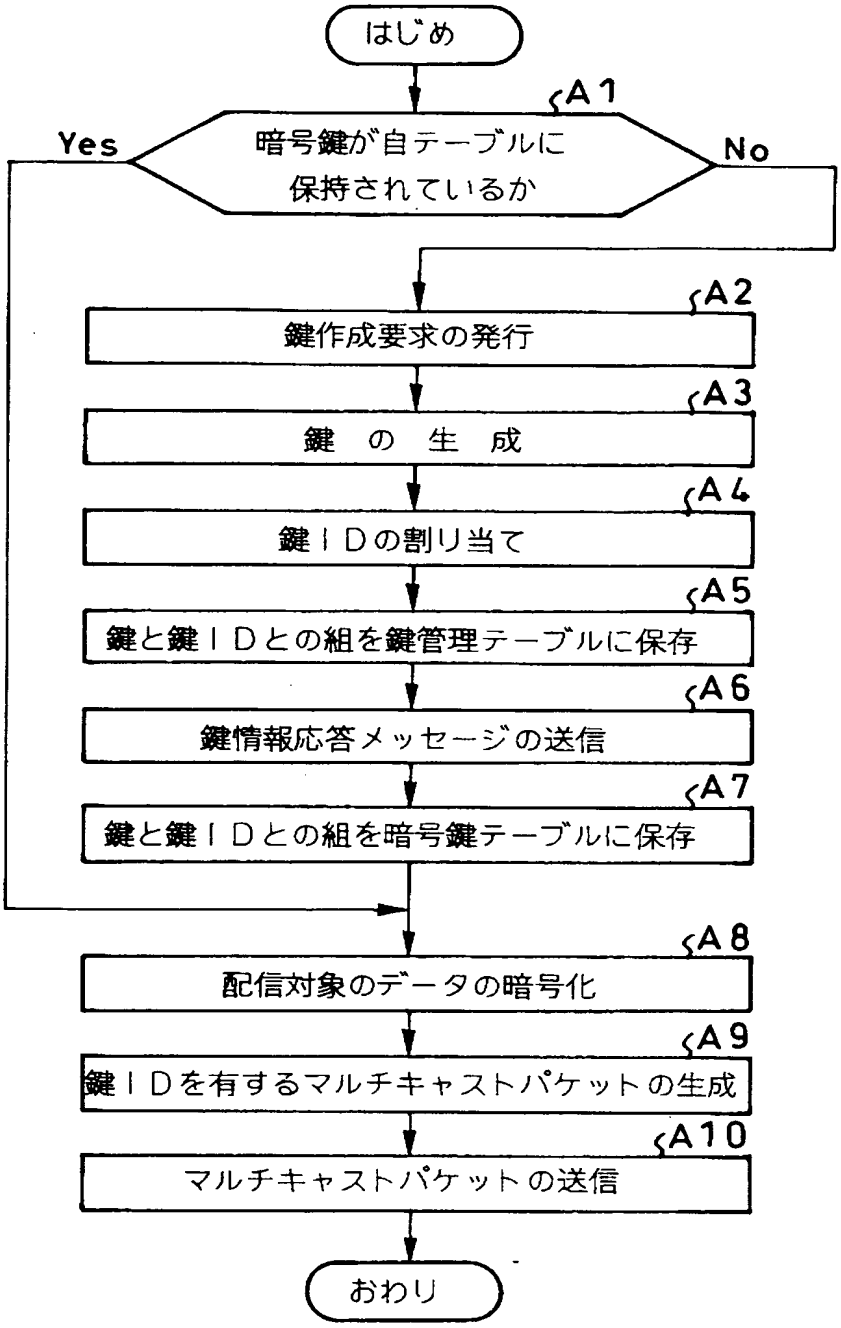
【図１】


312
復号鍵送付手段
310
鍵生成手段
鍵管理テーブル
311
鍵管理サーバ
31
1n0
1n
1n1
1n2
暗号鍵テーブル
コンテンツサーバ
暗号鍵取得手段
暗号化・送信手段
2m1
2m2
2m
2m0
復号鍵取得手段
受信・復号化手段
クライアント
復号鍵テーブル
120
12
121
122
221
222
22
220
110
11
111
112
211
212
21
210
100
ネットワーク
マルチキャストパケット
（暗号化データ＋鍵ＩＤ）

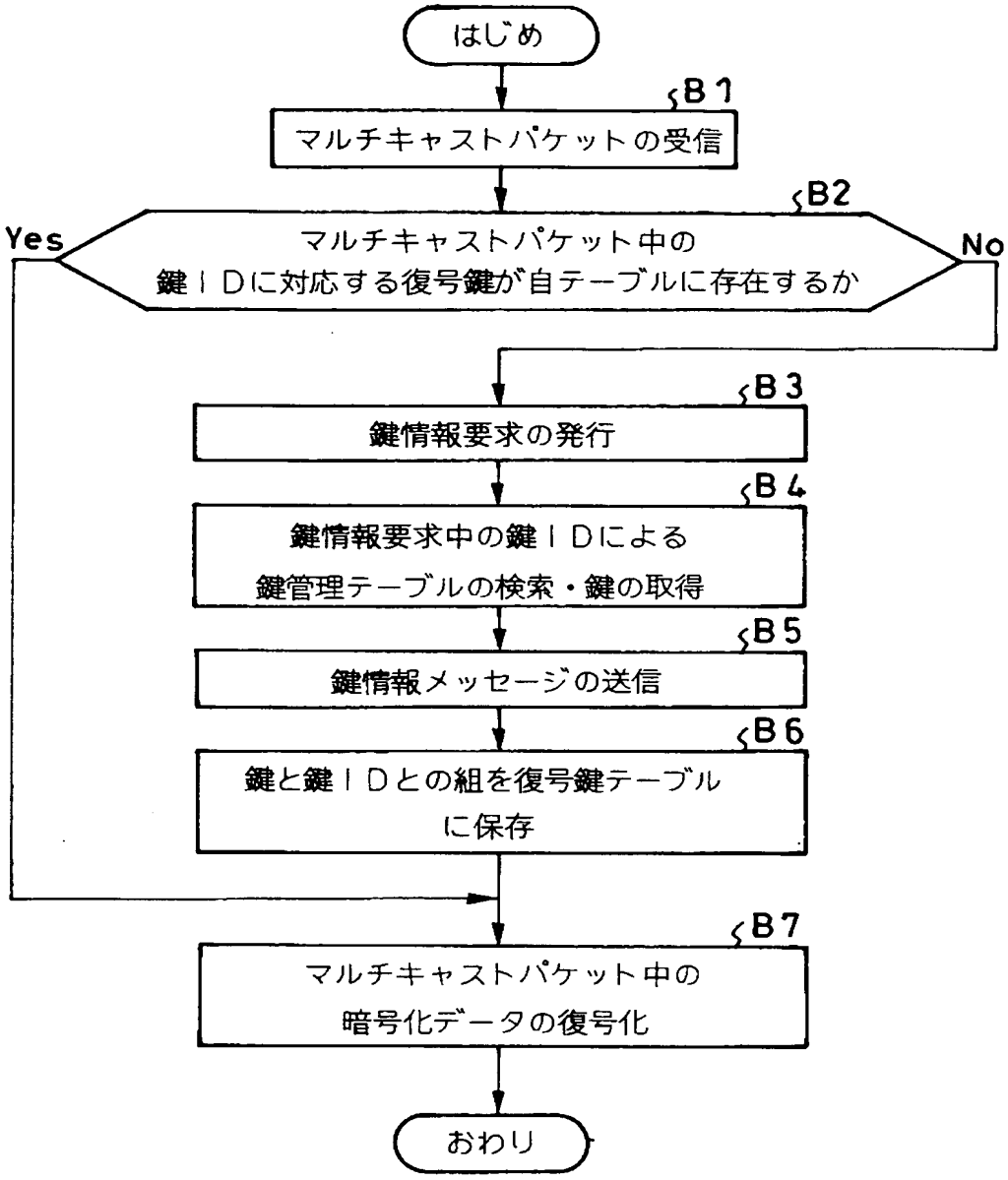
【図２】


鍵作成要求
鍵情報応答メッセージ（鍵ＩＤ＋鍵）
52
51
31
鍵管理サーバ
鍵ＩＤ１＋鍵（暗号鍵・復号鍵）
鍵ＩＤ２＋鍵
鍵ＩＤ３＋鍵
鍵ＩＤ４＋鍵
鍵ＩＤ５＋鍵
鍵ＩＤ６＋鍵
310鍵管理テーブル
鍵情報メッセージ（鍵ＩＤ＋鍵）
鍵情報要求（鍵ＩＤ＋要求）
62
61
1n0暗号鍵テーブル
鍵ＩＤ３＋鍵（暗号鍵）
1n
コンテンツサーバ
120暗号鍵テーブル
鍵ＩＤ４＋鍵（暗号鍵）
鍵ＩＤ２＋鍵
12
コンテンツサーバ
110暗号鍵テーブル
鍵ＩＤ１＋鍵（暗号鍵）
11
コンテンツサーバ
100
ネットワーク
マルチキャストパケット（暗号化データ＋鍵ＩＤ）
22
2m
クライアント
21
クライアント
クライアント
鍵ＩＤ１＋鍵（復号鍵）
鍵ＩＤ２＋鍵
鍵ＩＤ３＋鍵
鍵ＩＤ４＋鍵
210復号鍵テーブル
220復号鍵テーブル
2m0復号鍵テーブル

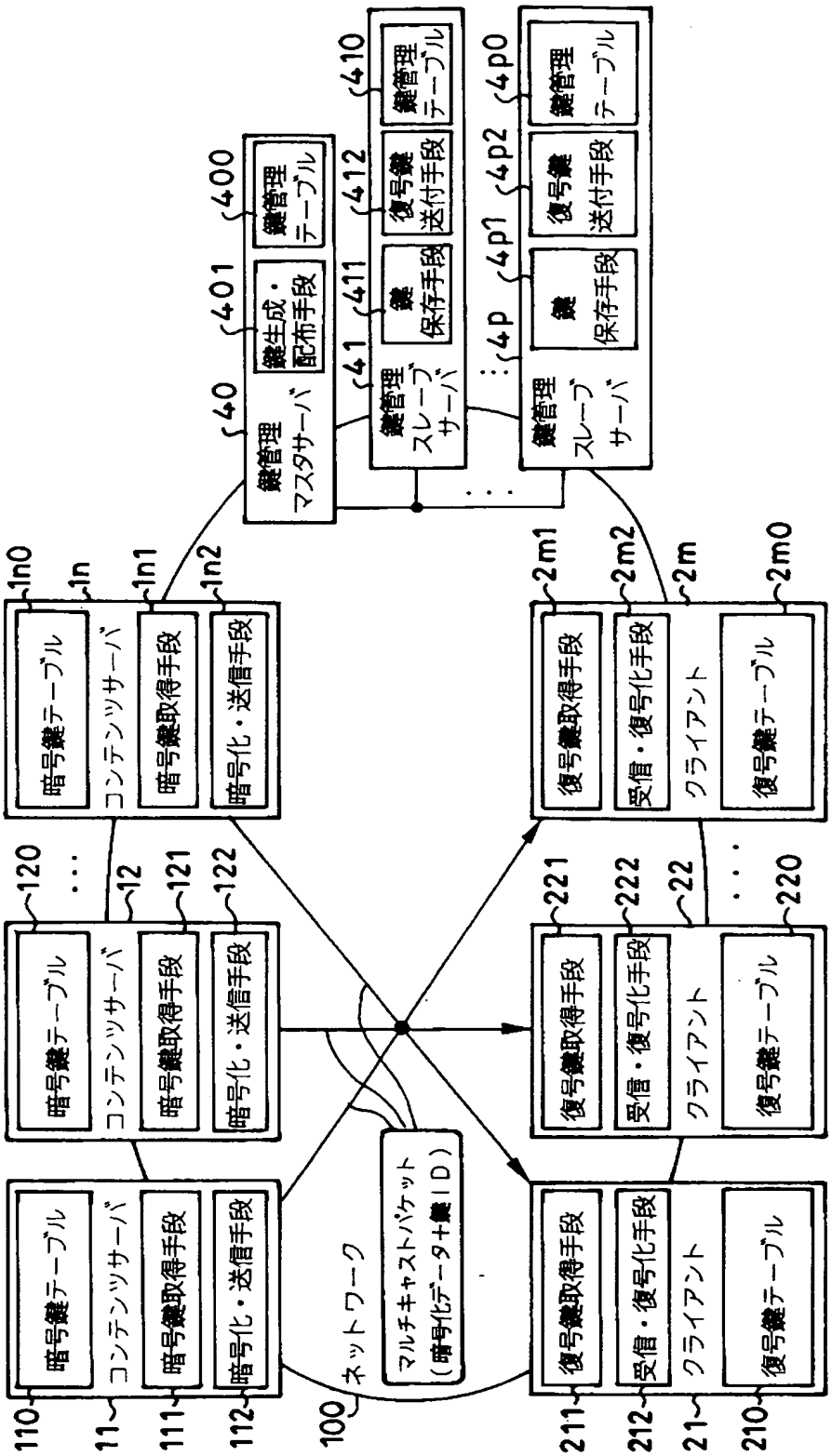
【図３】


はじめ
A1
暗号鍵が自テーブルに保持されているか
Yes
No
A2
鍵作成要求の発行
A3
鍵　の　生　成
A4
鍵ＩＤの割り当て
A5
鍵と鍵ＩＤとの組を鍵管理テーブルに保存
A6
鍵情報応答メッセージの送信
A7
鍵と鍵ＩＤとの組を暗号鍵テーブルに保存
A8
配信対象のデータの暗号化
A9
鍵ＩＤを有するマルチキャストパケットの生成
A10
マルチキャストパケットの送信
おわり

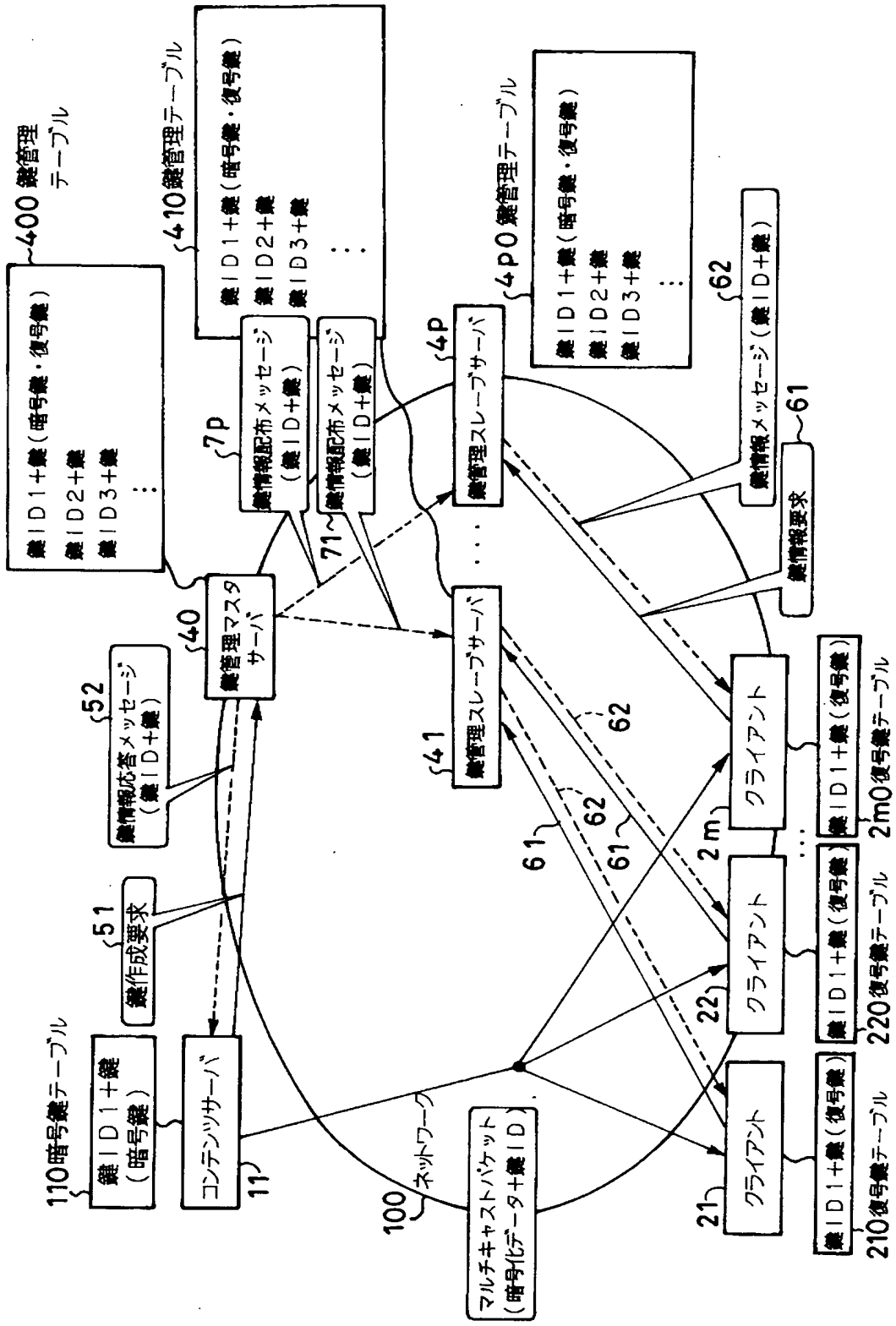
【図４】


はじめ
B1
マルチキャストパケットの受信
B2
Yes
マルチキャストパケット中の
鍵ＩＤに対応する復号鍵が自テーブルに存在するか
No
B3
鍵情報要求の発行
B4
鍵情報要求中の鍵ＩＤによる
鍵管理テーブルの検索・鍵の取得
B5
鍵情報メッセージの送信
B6
鍵と鍵ＩＤとの組を復号鍵テーブル
に保存
B7
マルチキャストパケット中の
暗号化データの復号化
おわり

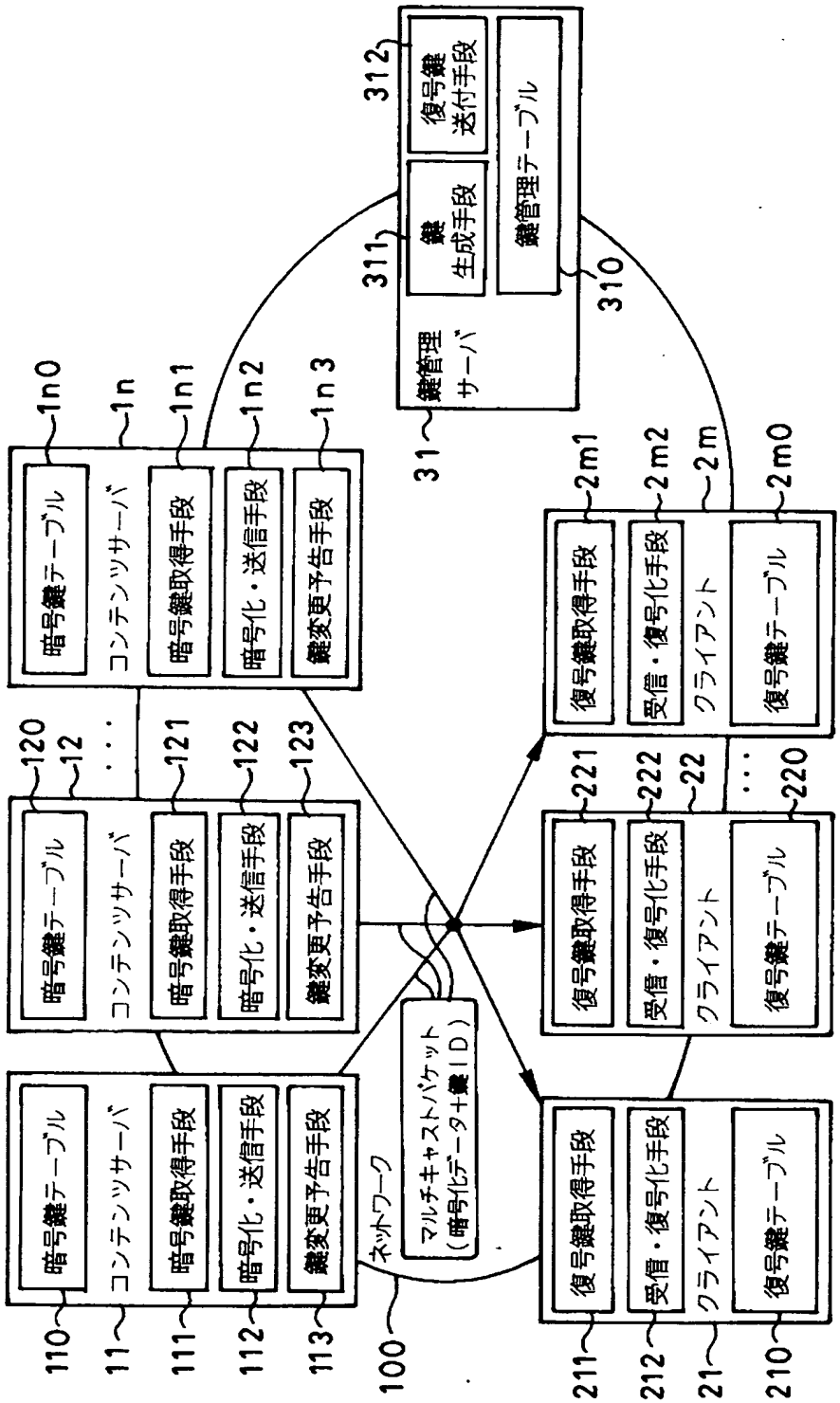
【図５】


鍵管理マスタサーバ
鍵生成・配布手段
鍵管理テーブル
鍵管理スレーブサーバ
鍵保存手段
復号鍵送付手段
鍵管理テーブル
コンテンツサーバ
暗号鍵テーブル
暗号鍵取得手段
暗号化・送信手段
クライアント
復号鍵取得手段
受信・復号化手段
復号鍵テーブル
ネットワーク
マルチキャストパケット
（暗号化データ＋鍵ＩＤ）
40
400
401
41
410
411
412
4p
4p0
4p1
4p2
1n0
1n
1n1
1n2
2m1
2m2
2m
2m0
120
12
121
122
221
222
22
220
110
11
111
112
100
211
212
21
210

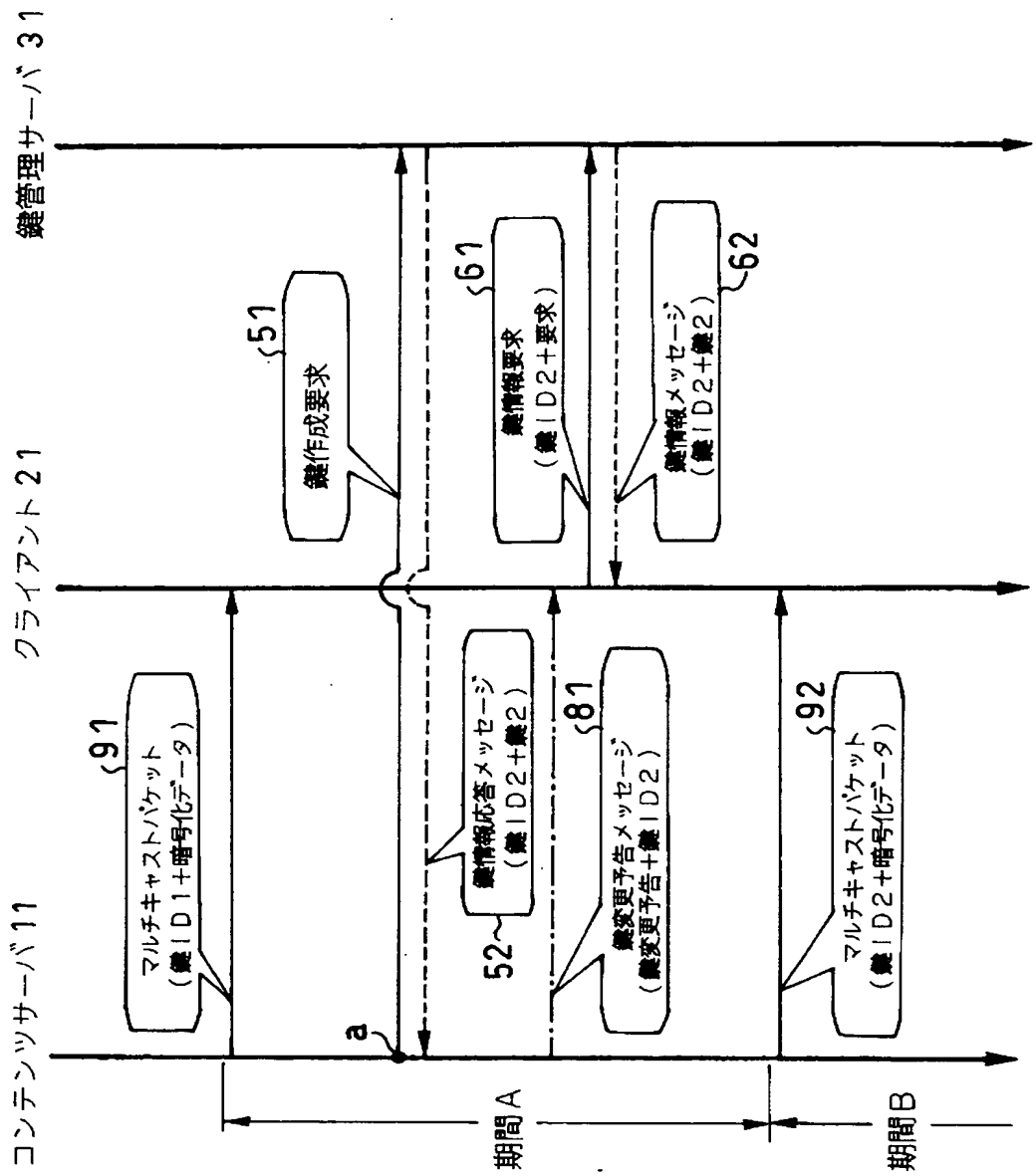
【図６】


400 鍵管理テーブル
鍵ＩＤ１＋鍵（暗号鍵・復号鍵）
鍵ＩＤ２＋鍵
鍵ＩＤ３＋鍵
410 鍵管理テーブル
鍵ＩＤ１＋鍵（暗号鍵・復号鍵）
鍵ＩＤ２＋鍵
鍵ＩＤ３＋鍵
4P0 鍵管理テーブル
鍵ＩＤ１＋鍵（暗号鍵・復号鍵）
鍵ＩＤ２＋鍵
鍵ＩＤ３＋鍵
鍵管理マスタサーバ
40
鍵管理スレーブサーバ
41
鍵管理スレーブサーバ
4P
鍵情報配布メッセージ（鍵ＩＤ＋鍵）
7P
71
鍵情報応答メッセージ（鍵ＩＤ＋鍵）
52
鍵作成要求
51
鍵情報要求
61
鍵情報メッセージ（鍵ＩＤ＋鍵）
62
110暗号鍵テーブル
鍵ＩＤ１＋鍵（暗号鍵）
コンテンツサーバ
11
ネットワーク
100
マルチキャストパケット（暗号化データ＋鍵ＩＤ）
クライアント
21
クライアント
22
クライアント
2m
鍵ＩＤ１＋鍵（復号鍵）
210復号鍵テーブル
鍵ＩＤ１＋鍵（復号鍵）
220復号鍵テーブル
鍵ＩＤ１＋鍵（復号鍵）
2m0復号鍵テーブル

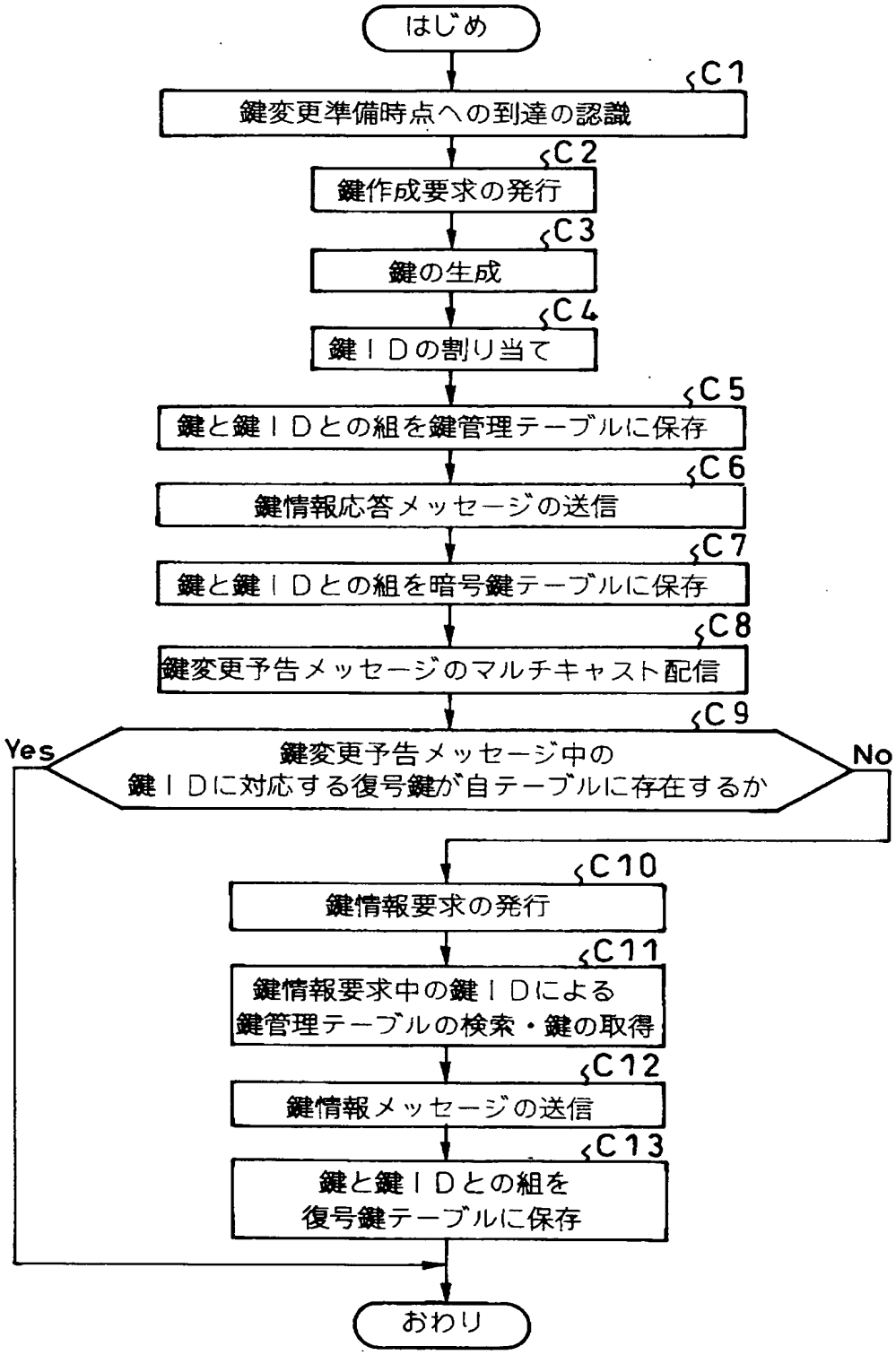
【図７】


312
復号鍵送付手段
311
鍵生成手段
鍵管理テーブル
鍵管理サーバ
31
310
1n0
1n
1n1
1n2
1n3
暗号鍵テーブル
コンテンツサーバ
暗号鍵取得手段
暗号化・送信手段
鍵変更予告手段
120
12
121
122
123
110
11
111
112
113
100
ネットワーク
マルチキャストパケット
（暗号化データ＋鍵ＩＤ）
2m1
2m2
2m
2m0
復号鍵取得手段
受信・復号化手段
クライアント
復号鍵テーブル
221
222
22
220
211
212
21
210

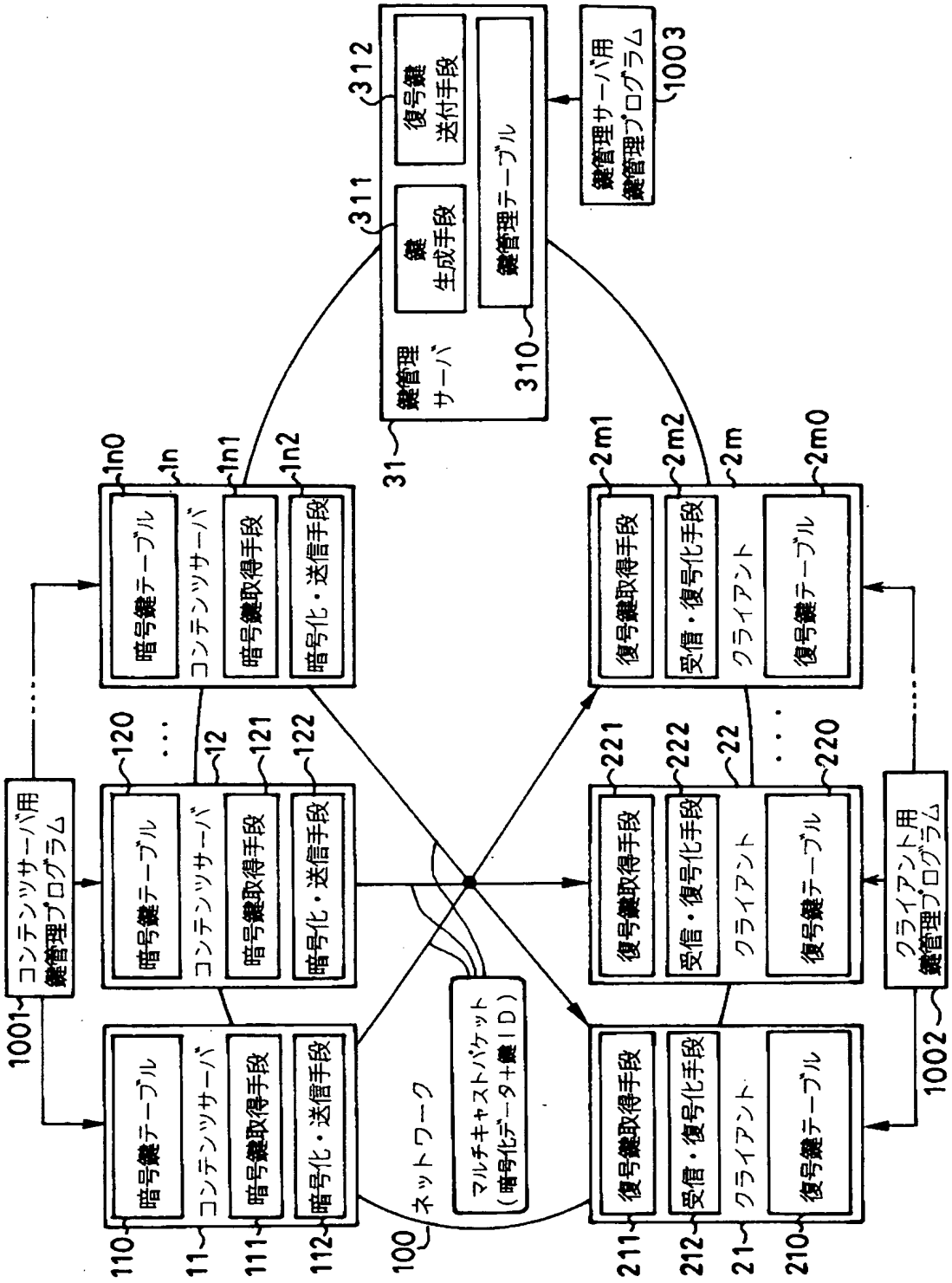
【図８】


鍵管理サーバ31
クライアント21
コンテンツサーバ11
鍵作成要求
51
鍵情報要求
（鍵ID2＋要求）
61
鍵情報メッセージ
（鍵ID2＋鍵2）
62
マルチキャストパケット
（鍵ID1＋暗号化データ）
91
鍵情報応答メッセージ
（鍵ID2＋鍵2）
52
鍵変更予告メッセージ
（鍵変更予告＋鍵ID2）
81
マルチキャストパケット
（鍵ID2＋暗号化データ）
92
a
期間A
期間B

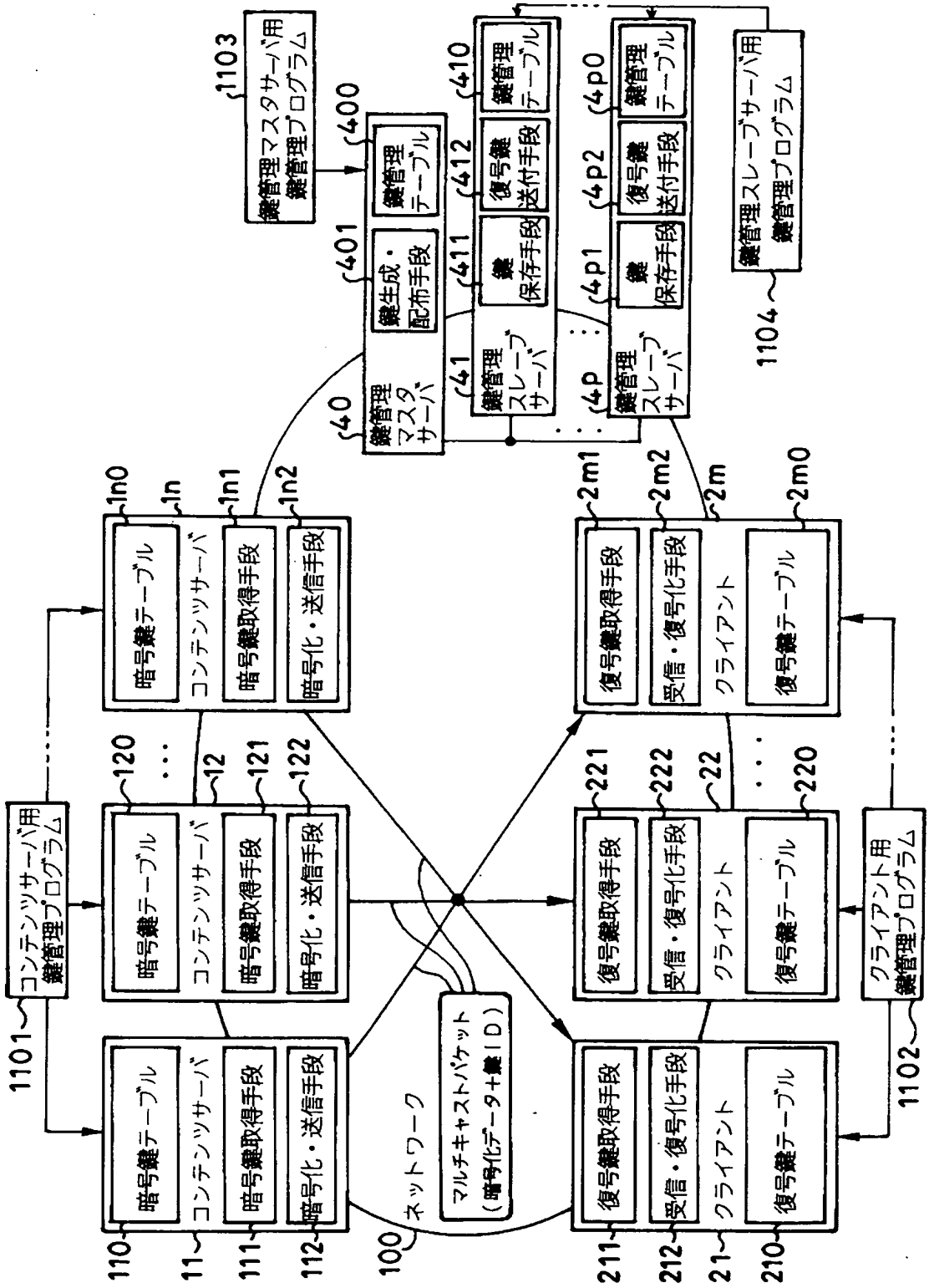
【図９】


はじめ
C1
鍵変更準備時点への到達の認識
C2
鍵作成要求の発行
C3
鍵の生成
C4
鍵ＩＤの割り当て
C5
鍵と鍵ＩＤとの組を鍵管理テーブルに保存
C6
鍵情報応答メッセージの送信
C7
鍵と鍵ＩＤとの組を暗号鍵テーブルに保存
C8
鍵変更予告メッセージのマルチキャスト配信
C9
鍵変更予告メッセージ中の
鍵ＩＤに対応する復号鍵が自テーブルに存在するか
Yes
No
C10
鍵情報要求の発行
C11
鍵情報要求中の鍵ＩＤによる
鍵管理テーブルの検索・鍵の取得
C12
鍵情報メッセージの送信
C13
鍵と鍵ＩＤとの組を
復号鍵テーブルに保存
おわり

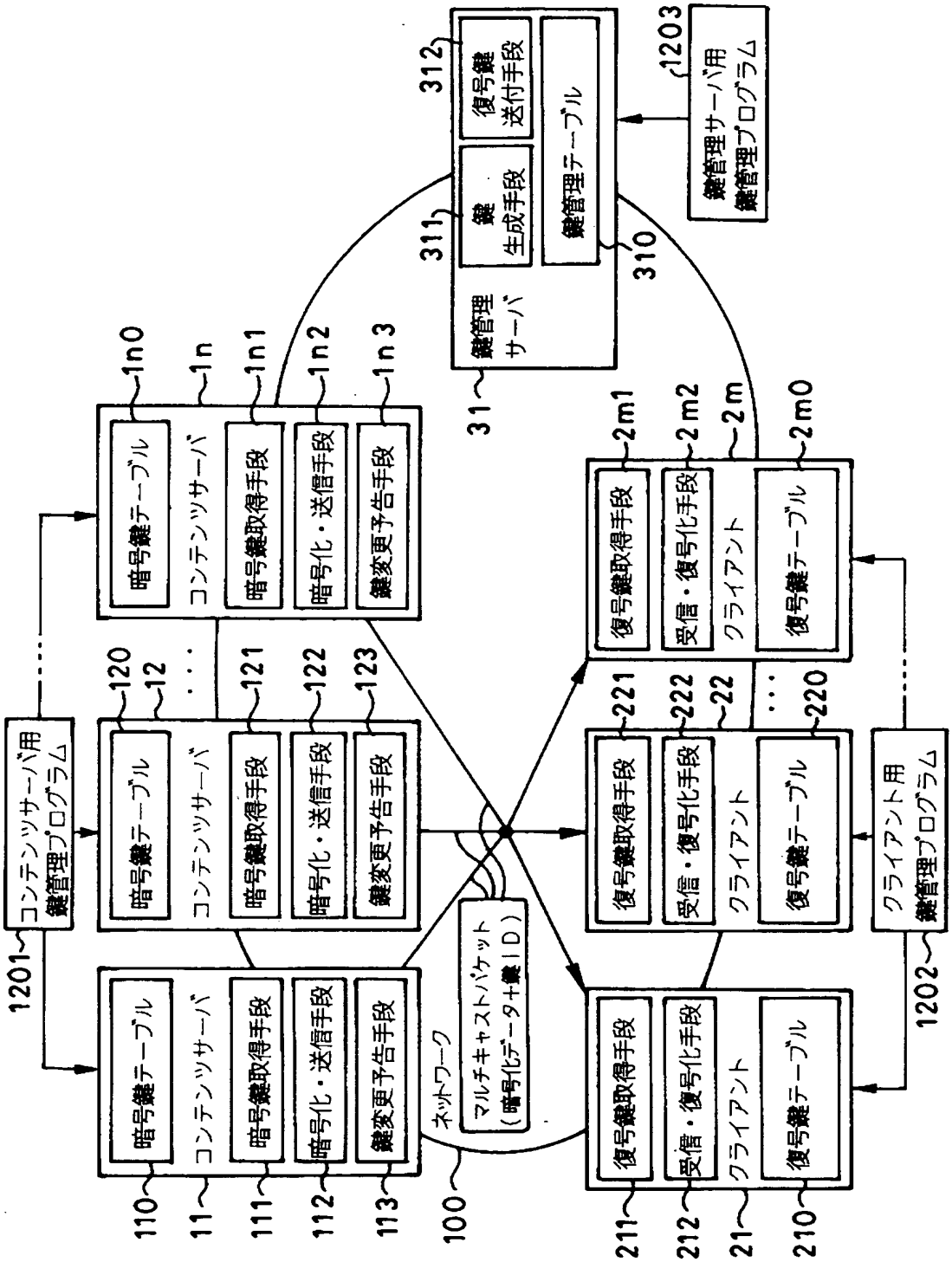
【図１０】


鍵管理サーバ用鍵管理プログラム
1003
鍵管理サーバ
31
鍵生成手段
311
復号鍵送付手段
312
鍵管理テーブル
310
コンテンツサーバ用鍵管理プログラム
1001
暗号鍵テーブル
1n0
コンテンツサーバ
1n
暗号鍵取得手段
1n1
暗号化・送信手段
1n2
暗号鍵テーブル
120
コンテンツサーバ
12
暗号鍵取得手段
121
暗号化・送信手段
122
暗号鍵テーブル
110
コンテンツサーバ
11
暗号鍵取得手段
111
暗号化・送信手段
112
ネットワーク
100
マルチキャストパケット
（暗号化データ＋鍵ＩＤ）
復号鍵取得手段
2m1
受信・復号化手段
2m2
クライアント
2m
復号鍵テーブル
2m0
復号鍵取得手段
221
受信・復号化手段
222
クライアント
22
復号鍵テーブル
220
復号鍵取得手段
211
受信・復号化手段
212
クライアント
21
復号鍵テーブル
210
クライアント用鍵管理プログラム
1002

【図１１】


鍵管理マスタサーバ用鍵管理プログラム
1103
鍵管理マスタサーバ
40
鍵管理テーブル
400
鍵生成・配布手段
401
鍵保存手段
411
復号鍵送付手段
412
鍵管理テーブル
410
鍵管理スレーブサーバ
41
鍵管理スレーブサーバ
4p
鍵保存手段
4p1
復号鍵送付手段
4p2
鍵管理テーブル
4p0
鍵管理スレーブサーバ用鍵管理プログラム
1104
コンテンツサーバ用鍵管理プログラム
1101
暗号鍵テーブル
コンテンツサーバ
暗号鍵取得手段
暗号化・送信手段
1n0
1n
1n1
1n2
暗号鍵テーブル
コンテンツサーバ
暗号鍵取得手段
暗号化・送信手段
120
12
121
122
暗号鍵テーブル
コンテンツサーバ
暗号鍵取得手段
暗号化・送信手段
110
11
111
112
ネットワーク
100
マルチキャストパケット
（暗号化データ＋鍵ID）
復号鍵取得手段
受信・復号化手段
クライアント
復号鍵テーブル
2m1
2m2
2m
2m0
復号鍵取得手段
受信・復号化手段
クライアント
復号鍵テーブル
221
222
22
220
復号鍵取得手段
受信・復号化手段
クライアント
復号鍵テーブル
211
212
21
210
クライアント用鍵管理プログラム
1102

【図１２】


コンテンツサーバ用鍵管理プログラム
1201
暗号鍵テーブル
コンテンツサーバ
暗号鍵取得手段
暗号化・送信手段
鍵変更予告手段
110
11
111
112
113
120
12
121
122
123
1n0
1n
1n1
1n2
1n3
ネットワーク
マルチキャストパケット（暗号化データ＋鍵ID）
100
鍵管理サーバ
311
鍵生成手段
鍵管理テーブル
310
31
312
復号鍵送付手段
1203
鍵管理サーバ用鍵管理プログラム
復号鍵テーブル
クライアント
復号鍵取得手段
受信・復号化手段
211
212
21
210
221
222
22
220
2m1
2m2
2m
2m0
クライアント用鍵管理プログラム
1202

【書類名】　要約書

【要約】

【課題】　暗号化データのマルチキャスト配信が行われるネットワークシステムにおける鍵（暗号鍵／復号鍵）の管理を容易に実現できるようにする。

【解決手段】　鍵管理サーバ３１は、暗号鍵・復号鍵と当該鍵を一意に識別するための鍵ＩＤとの組を保持することによって鍵を管理する。コンテンツサーバ１１～１ｎの各々は、鍵管理サーバ３１から暗号鍵とその鍵ＩＤとの組を受け取り、当該暗号鍵で暗号化されたデータと当該鍵ＩＤとを有するマルチキャストパケットをクライアント２１～２ｍに送信する。クライアント２１～２ｍの各々は、コンテンツサーバ１１～１ｎからマルチキャストパケットを受信し、当該マルチキャストパケットに含まれる鍵ＩＤに対応する復号鍵を鍵管理サーバ３１から取得し、当該復号鍵によって当該マルチキャストパケットに含まれる暗号化データの復号化を行う。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００２－３３２４０５
受付番号	５０２０１７３１５５９
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１４年１１月１８日

＜認定情報・付加情報＞

【提出日】　平成14年11月15日

次頁無

特願２００２－３３２４０５

出　願　人　履　歴　情　報

識別番号　　［０００００４２３７］

１．変更年月日　　１９９０年　８月２９日
［変更理由］　　新規登録
住　所　　東京都港区芝五丁目７番１号
氏　名　　日本電気株式会社